Затверджено
Завідувач кафедри УКБЗІ_____ С. Легомінова
“ 31 “ серпня 2026 р.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«АУДИТ СИСТЕМ 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/ODQzNzU0NjUyMDU1?hl=ru&cjc=xaz2o5bg	
Галузь знань			F «Інформаційні технології»		**Рівень вищої освіти**	перший (бакалаврський)	
Спеціальність			F5 «Кібербезпека та захист інформації»		**Семестр**	7	
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 необхідної системи знань з основ аудиту систем менеджменту інформаційної безпеки.

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 10.** Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційного простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Програмні результати навчання (РН)
РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційного простору й інформаційними ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Розділ 1 « БАЗОВІ ПОНЯТТЯ АУДИТУ СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»			
Тема 1. Основи функціонування систем менеджменту інформаційної безпеки ***Знати***: ключові поняття та визначення у сфері менеджменту інформаційної безпеки; структуру та основні елементи СМІБ (політика, організація, процеси, документи, ресурси); цілі та завдання СМІБ у контексті стратегії розвитку організації; категорії заходів забезпечення ІБ (організаційні, технічні, фізичні, кадрові); місце СМІБ в інтегрованій системі менеджменту та взаємозв'язок з іншими системами (ISO 9001, ISO 14001, ISO 45001); міжнародні та національні стандарти у сфері ІБ, зокрема вимоги ISO/IEC 27001 до планування, впровадження, підтримки та вдосконалення СМІБ. ***Вміти***: визначати внутрішній та зовнішній контекст організації при формуванні СМІБ; аналізувати фактори, що впливають на ефективність системи; визначати область застосування СМІБ з урахуванням специфіки діяльності; формулювати завдання та цілі інформаційної безпеки, що узгоджуються із загальною стратегією бізнесу; ідентифікувати необхідні документи для створення, підтримки та аудиту СМІБ (політики, процедури, регламенти, інструкції, плани реагування). ***Формування компетенцій:*** ІК, СК 10 ***Результати навчання:*** РН 21 ***Рекомендовані джерела:*** 1-31	Лекція 1 2 год	5	Лекція-візуалізація
	Практичне заняття 1 2 год		Практична робота: Аналіз вимог стандарту ISO/IEC 27001:2022 у контексті сертифікації СМІБ. Визначення складу та структури документації СМІБ (приклади політик, процедур, планів реагування).
	Самостійна робота		Огляд ключових стандартів у сфері ІБ: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005. Дослідження взаємодії СМІБ з іншими системами менеджменту (якість, охорона праці, екологія, безперервність). Класифікація категорій заходів інформаційної безпеки з прикладами впровадження. Огляд методів аналізу внутрішнього та зовнішнього контексту організації. Аналіз структури та змісту політики інформаційної безпеки на прикладі реальних компаній. Вивчення типових документів СМІБ: політики, процедури, регламенти, інструкції, плани реагування на інциденти.
Тема 2. Базові поняття та принципи аудиту інформаційної безпеки ***Знати***: загальні поняття та особливості проведення аудиту СМІБ; цілі та завдання аудиту у контексті забезпечення ІБ та управління ризиками; класифікацію аудитів: за типами, напрямками, масштабом; принципи проведення внутрішнього аудиту. ***Вміти***: визначати й формулювати цілі аудиту інформаційної безпеки відповідно до потреб і пріоритетів організації; обирати відповідний тип	Лекція 2 2 год	5	Лекція-візуалізація, експрес-опитування
	Практичне заняття 2 2 год		Практична робота: Формування цілей аудиту відповідно до потреб і стратегії організації. Відпрацювання способів дотримання принципів аудиту на прикладі кейсів.

аудиту залежно від ситуації та завдань; класифікувати аудити за різними ознаками та пояснювати відмінності між ними; застосовувати базові принципи аудиту на практиці. ***Формування компетенцій:*** ІК, СК 10 ***Результати навчання:*** РН 21 ***Рекомендовані джерела:*** 1-31	Самостійна робота		Дослідження відмінностей між типами аудитів за метою, методологією та результатами. Огляд і обґрунтування значення ключових принципів аудиту (незалежність, об'єктивність, компетентність тощо). Класифікація аудитів за напрямками: технічний, організаційний, процесний. Аналіз підходів до визначення цілей аудиту залежно від ризиків і стратегічних пріоритетів організації. Методи оцінки ефективності проведених внутрішніх аудитів: показники, метрики, Lessons Learned.
Тема 3. Управління програмою аудиту СМІБ ***Знати***: сутність та призначення програми аудиту і плану аудиту, їхню структуру, компоненти й цілі; настанови міжнародних стандартів ISO 19011 та ISO/IEC 27007 щодо планування й проведення аудитів систем управління; обов'язки та вимоги до компетентності особи, відповідальної за управління програмою аудиту; принципи ризик-орієнтованого планування аудиту; методи аналізу результатів і вдосконалення програми аудиту. ***Вміти***: аналізувати програму аудиту на відповідність міжнародним стандартам та потребам організації; оцінювати ризики й можливості, що виникають під час реалізації програми аудиту; визначати обсяг програми аудиту та планувати її реалізацію з урахуванням пріоритетів, ресурсів і строків; формулювати область застосування аудитів, ключові цілі, завдання та критерії оцінки; планувати та розраховувати ресурси (людські, фінансові, технічні) для виконання програми аудиту; здійснювати моніторинг і вдосконалення програми аудиту для підвищення її ефективності; оцінювати компетентність аудиторів і визначати необхідні навички та знання для виконання завдань. ***Формування компетенцій:*** ІК, СК 10 ***Результати навчання:*** РН 21 ***Рекомендовані джерела:*** 1-31	Лекція 3 2 год	5	Лекція-візуалізація, експрес-опитування
	Практичне заняття 3 2 год		Практична робота: Визначення обсягу програми аудиту на прикладі організації. Формування аудиторської команди та розподіл обов'язків.
	Самостійна робота		Аналіз підходів до планування та структуризації програми аудиту (з прикладами). Розробка плану аудиту: визначення області, цілей та обсягу. Дослідження ролі керівника програми аудиту, його обов'язків і компетенцій. Аналіз методів корекції програми аудиту на основі результатів попередніх перевірок. Планування та оптимізація ресурсів для реалізації програми аудиту. Вивчення кейсів управління програмами аудиту у міжнародних компаніях.
Розділ 2 «МЕТОДОЛОГІЯ ПРОВЕДЕННЯ АУДИТУ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ВІДПОВІДНІСТЬ ВИМОГАМ СТАНДАРТУ ISO/IEC 27001»			
Тема 4. Підготовчий етап аудиту СМІБ ***Знати***: перелік заходів, що здійснюються на етапі ініціювання та підготовки аудиту; вимоги до компетентності, обов'язків і ролей членів аудиторської команди; порядок підготовки, розподілу ролей і комунікації в команді аудиторів; рекомендації та вимоги ISO 19011 і	Лекція 4 2 год	5	Лекція-візуалізація

ISO/IEC 27007 щодо планування та підготовки аудиту; перелік документів, що мають бути зібрані й підготовлені до початку перевірки (політики, процедури, регламенти, звіти, записи). ***Вміти***: визначати й формулювати цілі та обсяг аудиту з урахуванням потреб організації й вимог стандартів; збирати та аналізувати попередню інформацію про організацію та її СМІБ для оцінки сфери аудиту; розробляти програму та детальний план аудиту (ключові завдання, терміни, ресурси, відповідальні особи); враховувати ризики й можливості, що можуть вплинути на підготовку та проведення аудиту; організовувати роботу аудиторської команди, забезпечувати відповідність компетенцій аудиторів вимогам; налагоджувати ефективну комунікацію з представниками організації, що перевіряється. ***Формування компетенцій:*** ІК, СК 10 ***Результати навчання:*** РН 21 ***Рекомендовані джерела:*** 1-31	Практичне заняття 4 2 год		Практична робота: Формування програми аудиту. Матриця компетентностей та розподіл ролей аудиторської команди. Ідентифікація ризиків підготовчого етапу аудиту.
	Самостійна робота		Аналіз прикладів програм аудиту з міжнародної практики. Розробка переліку документів, які необхідно підготувати перед аудитом. Дослідження ролі керівника аудиторської програми та вимог до його компетентності. Огляд типових помилок під час підготовки до аудиту СМІБ. Вивчення методів комунікації аудиторської команди з організацією, що перевіряється.
Тема 5. Перший етап аудиту СМІБ: підготовка, відвідування об'єкта та аналіз документації ***Знати***: завдання й цілі першого етапу аудиту СМІБ (ознайомлення з організацією, аналіз контексту, попередня оцінка готовності); методи збору інформації під час відвідування об'єкта (спостереження, інтерв'ю, аналіз записів); роль та відповідальність ключових зацікавлених сторін (керівництво, спеціалісти, персонал) у процесі аудиту; процедури аналізу документації СМІБ: політики, процедури, журнали, звіти, протоколи; вимоги до складання звіту за результатами першого етапу аудиту (структура, обов'язкові розділи, ключові висновки). ***Вміти***: організовувати й проводити візити до об'єктів аудиту, ефективно поєднуючи спостереження, інтерв'ю та аналіз даних; встановлювати професійні контакти із зацікавленими сторонами для отримання об'єктивної інформації; аналізувати документацію СМІБ на предмет відповідності вимогам ISO/IEC 27001:2022 та внутрішніх регламентів; оцінювати якість і повноту зібраних матеріалів; готувати звіт першого етапу аудиту з формулюванням ключових висновків, виявлених невідповідностей і рекомендацій для другого етапу. ***Формування компетенцій:*** ІК, СК 10 ***Результати навчання:*** РН 21 ***Рекомендовані джерела:*** 1-31	Лекція 5 2 год	5	Лекція-візуалізація, експрес-опитування
	Практичне заняття 5 2 год		Практична робота: Аналіз політик та процедур ІБ на відповідність стандарту ISO/IEC 27001. Оцінка ефективності управління доступом і контролю інформаційних активів (розбір кейсів: хто має доступ, як ведеться облік, чи є невідповідності).
	Самостійна робота		Огляд методів збору інформації під час відвідування об'єкта аудиту (порівняння ефективності: інтерв'ю, спостереження, аналіз документів). Визначення ключових зацікавлених сторін та методики встановлення контактів (з прикладами питань для інтерв'ю). Роль керівництва, ІТ-підрозділу та персоналу у першому етапі аудиту. Дослідження особливостей збору інформації в різних галузях (фінанси, охорона здоров'я, ІТ-сектор) та адаптація підхід для СМІБ. Приклади структури звіту за результатами першого етапу аудиту (обов'язкові розділи, висновки, рекомендації).

Тема 6. Другий етап аудиту СМІБ: проведення аудиту на місці та збір доказів ***Знати***: завдання і цілі другого етапу аудиту СМІБ; методи збору доказів на місці (інтерв'ю, спостереження, перевірка документів, вибіркове тестування процедур); процедури й інструменти для оцінки ефективності заходів та процесів ІБ; правила та етику проведення інтерв'ю (методи отримання достовірної інформації, уникнення упередженості, збереження об'єктивності); вимоги до структури й змісту звіту другого етапу аудиту (висновки, невідповідності, рекомендації). ***Вміти***: організовувати і проводити аудит на місці, планувати й координувати дії команди аудиторів; застосовувати техніки збору доказів для оцінки відповідності СМІБ стандартам та внутрішнім вимогам; оцінювати ефективність заходів ІБ, виявляти сильні сторони та слабкі місця системи; проводити інтерв'ю з персоналом, отримуючи достовірну інформацію про процеси та практики; документувати результати другого етапу аудиту у вигляді звіту; вирішувати конфліктні ситуації та непорозуміння під час аудиту, зберігаючи професіоналізм і неупередженість. ***Формування компетенцій:*** ІК, СК 10 ***Результати навчання:*** РН 21 ***Рекомендовані джерела:*** 1-31	Лекція 6 2 год	5	Лекція-візуалізація, експрес-опитування
	Практичне заняття 6 2 год		Практична робота: Аналіз методів збору аудиторських доказів (кейси: які дані вважати доказами, а які – припущеннями). Оцінка ефективності заходів реагування на інциденти: моделювання інциденту та аналіз дій організації.
	Самостійна робота		Методи збору аудиторських доказів: інтерв'ю, спостереження, перевірка документів – порівняння їхньої надійності. Розробка сценаріїв проведення інтерв'ю під час аудиту: питання, етика, способи уникнення упередженості. Документування результатів аудиту: структура, ключові елементи та формулювання висновків. Вирішення проблемних ситуацій під час аудиту: аналіз практичних кейсів (конфліктні відповіді, неповні документи, відсутність доступу). Розробка прикладу фрагменту звіту за результатами другого етапу аудиту.
Тема 7. Формування висновків і завершення аудиту СМІБ ***Знати***: етапи формування висновків за результатами аудиту; методи оцінки ефективності заходів і процедур у межах СМІБ; процедури завершення аудиту: підготовка фінального звіту, обговорення результатів, оформлення рекомендацій; вимоги стандартів до структури та змісту аудиторського звіту; правила професійної комунікації з клієнтами та зацікавленими сторонами після завершення аудиту; практики моніторингу виконання рекомендацій. ***Вміти***: аналізувати зібрані докази та формулювати на їх основі обгрунтовані висновки; готувати фінальний звіт із чіткою структурою	Лекція 7 2 год	5	Лекція-візуалізація, експрес-опитування
	Практичне заняття 7 2 год		Практична робота: Методи використання вибірок для аналізу аудиторських доказів (робота з умовними прикладами документів і записів). Практичний аналіз результатів аудиту та складання фрагмента фінального звіту (виявлені проблеми + рекомендації).

(невідповідності, оцінка ризиків, рекомендації); проводити презентацію результатів аудиту та забезпечувати конструктивний діалог з організацією; розробляти практичні рекомендації для вдосконалення СМІБ; організовувати процедури моніторингу виконання рекомендацій; вирішувати проблеми та непорозуміння, що виникають у процесі завершення аудиту. ***Формування компетенцій:*** ІК, СК 10 ***Результати навчання:*** РН 21 ***Рекомендовані джерела:*** 1-31	Самостійна робота		Структура та оформлення фінального звіту про аудит: вимоги ISO/IEC 27007 та ISO 19011. Техніки ефективної комунікації результатів аудиту з керівництвом та персоналом. Розробка рекомендацій для вдосконалення СМІБ (аналіз прикладів). Методи моніторингу реалізації рекомендацій після аудиту. Сценарії завершення аудиту: типові труднощі та шляхи їх подолання. Розробка плану вдосконалення СМІБ на основі висновків аудиту.
Розділ 3 «СПЕЦІАЛІЗОВАНІ АУДИТИ ТА СЕРТИФІКАЦІЙНІ ПРАКТИКИ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ»			
Тема 8. Тестування методами соціальної інженерії ***Знати***: основи соціальної інженерії та її вплив на ІБ; методи соціоінженерних атак (фішинг, вішинг, смішинг, шолдер-серфінг, tailgating тощо); способи використання соціальної інженерії як методу виявлення вразливостей у СМІБ; етапи проведення тестів на соціальну інженерію (планування, сценарії, виконання, аналіз); правові та етичні аспекти тестування соціальною інженерією (відповідальність аудитора, згоди, обмеження); вимоги до документування та звітності за результатами аудиту соціоінженерними методами. ***Вміти:*** планувати та проводити тестування інформаційної безпеки методами соціальної інженерії; розробляти сценарії та стратегії соціоінженерних атак для аудиту (з урахуванням цілей і ризиків організації); застосовувати різні види соціоінженерних атак у контрольованих умовах для оцінки захищеності; аналізувати результати тестів, виявляти вразливості та формувати рекомендації; оцінювати ефективність існуючих заходів захисту; дотримуватись правових та етичних норм, готувати професійні звіти з чітким описом результатів і рекомендацій. ***Формування компетенцій:*** ІК, СК 10 ***Результати навчання:*** РН 21 ***Рекомендовані джерела:*** 1-31	Лекція 8 2 год	5	Лекція-візуалізація
	Практичне заняття 8 2 год		Практична робота: Розробка програми підвищення обізнаності персоналу щодо соціальної інженерії. Аналіз кейсів успішних соціоінженерних атак на організації: помилки, наслідки, уроки.
	Самостійна робота		Соціальна інженерія та її вплив на організації: реальні інциденти та уроки. Методи навчання і підвищення обізнаності співробітників: тренінги, симуляції, фішинг-тести. Правові та етичні аспекти аудиту з використанням соціальної інженерії. Огляд і оцінка інструментів тестування соціоінженерних атак. Соціальна інженерія у цифрову епоху: нові виклики (DeepFake, AI-driven phishing). Типові помилки компаній у протидії соціальній інженерії та як їх уникнути. Розробка рекомендацій для вдосконалення політики безпеки на основі результатів соціоінженерного аудиту.
Тема 9. Сертифікаційні аудити: PCI DSS та NIST CSF ***Знати***: основні вимоги та цілі сертифікації PCI DSS та NIST CSF; процес сертифікації PCI DSS: підготовка, аудит, періодичність перевірок; процес впровадження та оцінювання за NIST CSF: методи самооцінки, рівні зрілості; ролі та обов'язки організацій у процесі	Лекція 9 2 год	5	Лекція-візуалізація
	Практичне заняття 9 2 год		Практична робота: Моделювання процесу сертифікації PCI DSS. Аналіз ролі BCMS (Business Continuity Management System) як складової забезпечення відповідності стандартам.

сертифікації; види документації, необхідної для сертифікації, та вимоги до звітів про відповідність. ***Вміти***: розробляти план підготовки до сертифікації PCI DSS і NIST CSF, визначаючи ресурси та етапи; проводити внутрішні аудити для перевірки відповідності вимогам стандартів; ідентифікувати вразливості, що можуть перешкоджати сертифікації; готувати документацію; взаємодіяти з аудиторами та сертифікаційними органами; аналізувати результати сертифікаційних аудитів і впроваджувати рекомендації; підтримувати постійну відповідність. ***Формування компетенцій:*** ІК, СК 10 ***Результати навчання:*** РН 21 ***Рекомендовані джерела:*** 1-31	Самостійна робота		Документація та звітність у сертифікації PCI DSS: структура та вимоги. Сертифікація PCI DSS у малих і середніх підприємствах: виклики та шляхи вирішення. Оцінка ефективності PCI DSS у захисті платіжних даних (аналіз реальних інцидентів). Інтеграція NIST CSF у бізнес-процеси організації: методологія та рекомендації. Ризики та проблеми при впровадженні NIST CSF у різних секторах (фінанси, державний сектор, IT). Порівняльний аналіз PCI DSS та NIST CSF: відмінності, переваги та сфери застосування.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Навчальна лабораторія «Центр управління інформаційною та кібернетичною безпекою» («Security Operation Center»).
- 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. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України редакція від 04 липня 2020 р. № 80/94-ВР / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
2. Про основні засади забезпечення кібербезпеки України : Закон України редакція від 24 жовтня 2020 р. № 2163-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
3 Про національну безпеку України : Закон України редакція від 24 жовтня 2020 р. № 2469-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355
4. Про заходи щодо захисту інформаційних ресурсів держави : Указ Президента України №582/2000 від 10.04 2000 р. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/582/2000#Text.
5. НД ТЗІ 3.1-003-2005. Порядок проведення робіт із створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf
6. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf
7. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 24.04.1999 р. № 22 Чинний від 01.07.1999 р. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf
8. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТЗІ СБ України від 04.12.2000 р. № 53 Чинний від 15.12.2000 р. URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf
9. Інформаційна безпека інформаційно-комунікаційних систем. Комплекси засобів захисту інформації від НСД. URL: http://www.dut.edu.ua/uploads/l_489_79827499.pdf
10. Рой Я.В., Мазур Н.П., Складанній П.М. Аудит інформаційної безпеки – основа ефективного захисту підприємств./ Кібербезпека: освіта, наука, техніка №1(1) - Київ: Київський університет імені Бориса Грінченка, 2018 с.87-93. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/23

11. ДСТУ ISO/IEC 27007:2018 (ISO/IEC 27007:2017, IDT) Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою
12. ДСТУ ISO 19011:2019 (ISO 19011:2018, IDT) Настанови щодо проведення аудитів систем управління
13. Інформаційні технології в бізнесі. Частина 1: Навч. посіб. / [Шевчук І.Б., Старух А.І., Васьків О.М. та ін.]; за заг. ред. І.Б. Шевчук. Львів: Видавництво ННВК «АТБ», 2020. 455 с. URL: https://financial.lnu.edu.ua/wp-content/uploads/2020/11/Posibnyk_IT-v-biznesi_2.pdf
14. Manual of Information Technology Audit. URL: https://cag.gov.in/uploads/media/ITAM-Vol-I-20210331113105.pdf
15. Information Security Audit (IT Audit / IS Audit). URL: https://youtu.be/fQefScHAs6A
16. Day 3: Security Auditing and Compliance. URL: https://youtu.be/O_noXhQ16Yk
17. Learn how to become great Cybersecurity Auditors and Consultants. URL: https://youtu.be/R6p4m5TGgik
18. How to Perform an Internal Network Audit. URL: https://youtu.be/-REmXQKzcCw
19. How to carry out an IT Infrastructure Audit. URL: https://youtu.be/kHkCNi0B4VY
Постанови Кабінету Міністрів України:
20. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури (від 19.06.2019 № 518)
21. Про затвердження Положення про організаційно-технічну модель кіберзахисту (від 29.12.2021 № 1426)
22. Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури(від24.03.2023 № 257)
23. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі (від 04.04.2023 № 299)
24. Деякі питання функціонування Національного центру резервування державних інформаційних ресурсів (від 07.04.2023 № 311)
25. Деякі питання створення та функціонування державних електронних платформ для ведення публічних електронних реєстрів (від 18.04.2023 № 356)
26. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-кмунікаційних систем, електронних комунікаційних мереж (від 16.05.2023 № 497)
Накази Адміністрації Держспецзв'язку:
27. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (від 06.10.2021 № 601, в редакції наказу від 10.07.2022 № 343)
28. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами (від 29.05.2023 № 463)
29. Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі (від 03.07.2023 № 570)
30. Якименко Ю.М., Рабчун Д.І., Мужанова Т.М., Запорожченко М.М., Щавінський Ю.В. Технічний аудит захищеності інформаційно-телекомунікаційних систем підприємства. *Кібербезпека: освіта, наука, техніка*. 2023. Том 4, № 20. С. 45-61. URL: https://doi.org/10.28925/2663-4023.2023.20.4561
31. Svitlana Lehominova, Mykhailo Zaporozhchenko, Yurii Shchavinsky, Tetiana Muzhanova, Vitalii Tyshchenko, Matvii Yushchenko. Methodology for determining means of monitoring information security by the method of expert assessment. International Journal of Computing. 2024. Vol. 23, № 4. P. 681-691. URL: https://doi.org/10.47839/ijc.23.4.3770

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 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 3 бали
РУБІЖНЕ ОЦІНЮВАННЯ	Розділ № 1 «БАЗОВІ ПОНЯТТЯ АУДИТУ СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»	максимальна оцінка – 15 балів
	Розділ № 2 «МЕТОДОЛОГІЯ ПРОВЕДЕННЯ АУДИТУ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ВІДПОВІДНІСТЬ ВИМОГАМ СТАНДАРТУ ISO/IEC 27001»	максимальна оцінка – 20 балів
	Розідл № 3 «СПЕЦІАЛІЗОВАНІ АУДИТИ ТА СЕРТИФІКАЦІЙНІ ПРАКТИКИ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ»	максимальна оцінка – 10 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	**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)

	тлумаченні теоретичних положень чи складних практичних завдань.		
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 допущеніпомилки, 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*

ПОЛІТИКА ДОБРОЧЕСНОСТІ

Здобувач вищої освіти виконуючи самостійну або індивідуальну роботу повинен дотримуватись політики доброчесності. У разі наявності плагіату в будь-яких видах робіт здобувача, він отримує незадовільну оцінку і повинен повторно виконати завдання, які передбачені у Силабусі.