Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
Кафедра теоретичної та прикладної системотехніки

"ЗАТВЕРДЖУЮ"
Проректор
з наукової-педагогічної роботи
_____ Олександр ГОЛОВКО
_____ 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Моніторинг та аудит інформаційно-аналітичних систем

рівень вищої освіти другий (магістерський) рівень

галузь знань 12 «Інформаційні технології»

спеціальність 123 «Комп'ютерна інженерія»

освітня програма «Комп'ютерна інженерія»

вид дисципліни вибіркова

факультет Комп'ютерних наук

2022 / 2023 навчальний рік

Програму обговорено та рекомендовано до затвердження вченою радою факультету комп’ютерних наук
«28» червня 2022 року, протокол №10

Програму схвалено на засіданні кафедри теоретичної та прикладної системотехніки
Протокол від «11» червня 2022 року, №12

Завідувач кафедри теоретичної та прикладної системотехніки
_____ Сергій ШМАТКОВ.

Програму погоджено з гарантом освітньої програми «Комп'ютерна інженерія»

Гарант освітньої програми «Комп'ютерна інженерія»
_____ Олена ТОЛСТОЛУЗЬКА

Програму погоджено методичною комісією факультету комп’ютерних наук
Протокол від «24» червня 2022 року № 9

Голова методичної комісії факультету комп’ютерних наук
_____ Анатолій БЕРДНІКОВ
підпис

ВСТУП

Програма навчальної дисципліни «Моніторинг та аудит інформаційно-управляючих систем» укладено відповідно до освітньо-професійних програм підготовки **другого (магістерського) рівня** вищої освіти за спеціальностями 123 «Комп'ютерна інженерія».

1. Опис навчальної дисципліни

1.1. Мета викладання навчальної дисципліни

Метою викладання дисципліни «Моніторинг та аудит інформаційно-управляючих систем» є – засвоєння студентами знань про процедури та інструменти проведення аудиту інформаційно-управляючих систем, формування навичок з аналізу та оцінки результатів моніторингу інформаційної безпеки, розробки результативних заходів IT-контролю, а також підготовки корпоративних планів розвитку автоматизованих систем.

1.2. Основні завдання вивчення дисципліни

Основними завданнями вивчення дисципліни є:

– основних понять аудиту та моніторингу інформаційно-управляючих систем;
– процесного підходу до організації інформаційної безпеки;
– основних вимог до змісту аудиту інформаційних систем;
– основ контролю та перевірки управляючих процесів та систем;
– процесу комплексного обстеження та методів оцінювання інформаційної безпеки;
– стандартів та нормативів професійної практики IT-аудиту.

В ході вивчення дисципліни у студента повинні формуватися наступні компетентності:

Загальні компетентності (ЗК):

– ЗК01. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;
– ЗК04. Здатність до пошуку, оброблення та аналізу інформації з різних джерел;
– ЗК07. Здатність розробляти проекти і управляти ними.

Спеціальні (фахові, предметні) компетентності (ФК):

– ФК02. 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 з метою здійснення професійної діяльності в галузі комп'ютерної інженерії;
– ФК04. Здатність застосовувати системний підхід до вирішення науково-технічних завдань комп'ютерної інженерії;
– ФК 05. Здатність досліджувати, розв'язувати складні професійні завдання і проблеми на основі розуміння технічних аспектів забезпечення контролю якості продукції;
– ФК07. Здатність застосовувати комплексний підхід до вирішення експериментальних завдань модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

1.3. Кількість кредитів – 6

Організація навчання у ЗВО України здійснюється за кредитно-трансферною накопичувальною системою, у зв'язку із чим навчальним планом факультету комп'ютерних наук на дисципліну «Моніторинг та аудит інформаційно-управляючих систем» виділено 6 кредити у першому навчальному семестрі.

1.4. Загальна кількість годин

180 годин

1.5. Характеристика навчальної дисципліни	
Вибіркова	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
1-й	1-й
Семестр	
1-й	1-й
Лекції	
32 год.	32 год.
Практичні, семінарські заняття	
16 год.	16 год.
Лабораторні заняття	
0 год.	0 год.
Самостійна робота	
132 год.	132 год.
у тому числі індивідуальні завдання	
0 год.	

1.6. Заплановані результати навчання

Відповідно до вимог освітньо-професійної програми студенти повинні досягти таких результатів навчання:

знати:

– основні поняття аудиту інформаційних систем та інформаційної безпеки;

– методи аналізу та оцінки захищеності автоматизованих інформаційних систем;

– національні та міжнародні стандарти в галузі проведення IT-аудиту та оцінки безпеки інформаційних систем;

– правові основи аудиту інформаційних систем;

– етапи та процедури аудиту інформаційно-управляючих систем;

– перелік можливих загроз інформаційній безпеці та шляхи їх подолання;

– основи управління IT-проектами;

– методологію стратегічного планування інформаційної безпеки;

– методи первинної оцінки відмовостійкості систем інформаційної безпеки;

– методи побудови безпечних інформаційних систем;

– основи контролю процесів в інформаційних системах;

– етапи процесу комплексного обстеження інформаційних систем комерційних підприємств;

уміти:

– досліджувати отримані оцінки інформаційної безпеки;

– оцінювати результати IT-аудиту;

– розрізняти типи загроз інформаційні безпеці

– використовувати процесний підхід до організації інформаційної безпеки;

– використовувати відомі методи кількісної оцінки показників інформаційної безпеки;

– підготовлювати звіт з висновками ІТ-аудиту та можливими рекомендаціями з підвищення інформаційної безпеки;

придбати навички:

– розробки компонентів систем інформаційної безпеки;

– застосування нормативних документів, стандартів при проведення ІТ-аудиту;

мати уявлення:

– про особливості проведення ІТ-аудиту в європейських країнах;

– про особливості побудови моделей безпечних інформаційних систем в залежності від масштабу бізнес-процесів.

В результаті вивчення дисципліни у студента повинні формуватися наступні програмні результати навчання (ПРН):

– ПРН01. Знати і розуміти сучасні методи наукових досліджень, організації та планування експерименту, збирання даних та моделювання в комп'ютерних системах;

– ПРН02. Знати і розуміти наукові і математичні положення, що лежать в основі функціонування програмних і програмно-технічних комп'ютерних засобів, систем та мереж, Інтернету речей, систем для оброблення великих даних;

– ПРН 06. Мати фундаментальні знання і розуміння моделей, а також технологій створення та використання прикладного і спеціалізованого програмного забезпечення розв'язування професійних задач і проблем комп'ютерної інженерії;

– ПРН 09. Вміти застосовувати знання для аналізу інженерних продуктів, процесів і систем за встановленими критеріями, ідентифікації, формулювання і розв'язування науково-технічних задач комп'ютерної інженерії, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей;

– ПРН13. Вміти розробляти нормативно-технічні документи та стандарти в області комп'ютерної інженерії на програмні, інженерні продукти, процеси і системи.

2. Тематичний план навчальної дисципліни

Розділ 1. Практична методологія ІТ-аудиту

Тема 1. Вступ: актуальність ІТ-аудиту, завдання ІТ-аудитора

Передумови виникнення та етапи розвитку концепції ІТ-аудиту. ІТ-аудит як ключовий компонент забезпечення якості інформаційних систем. Узагальнена класифікація видів ІТ-аудитів. Нормативно-правове забезпечення ІТ-аудиту. Термінологія та основні поняття ІТ-аудиту.

Тема 2. Об'єкти та межі аудиту інформаційних систем

Типові фактори ризику в аудиті інформаційних систем. Аспекти якості ІТ-аудиту. Рівні ІТ-аудиту. Результативність структури та операційні результативність заходів аудиту та моніторингу інформаційних систем. ІТ-аудит в державних установах.

Тема 3. Заходи контролю інформаційних систем

Загальні заходи контролю. Заходи контролю за прикладними програмами. Середовище застосування заходів контролю. Цілі заходів контролю. Заходи контролю щодо цілісності даних. Заходи контролю щодо обробки та видачі даних. Технології моніторингу заходів контролю.

Тема 4. Критерії IT-аудиту

Загальні та спеціальні критерії IT-аудиту. Доступність критеріїв IT-аудиту. Норми та стандарти проведення IT-аудиту (ISO/IEC12 27001 і 27002, COBIT 5, ITIL V3, ASL, PRINCE 2).

Тема 5. Інструменти і прийоми комп'ютеризованої підтримки аудиту (CAATTs)

Інструменти: NMAP, OWASP ZAP, Splunk, Flexicon Disco, Qlikview. Приклади використання інструментів IT-аудиту.

Розділ 2. Оцінка інформаційної безпеки управляючих систем

Тема 6. Моделювання інформаційної безпеки

Компоненти BMIS (організація, люди, технології, процеси). Динамічні взаємозв'язки між компонентами (інформаційні технології, архітектура систем різного призначення, культура, управління, людський фактор).

Тема 7. Моделі ідентифікації поточного стану інформаційної безпеки

Модель Threat and Risk Assessment (TRA).

Тема 8. Визначення факторів, які впливають на стан інформаційної безпеки

Методи визначення ступеню взаємозв'язків між факторами та їх влив на стан інформаційної безпеки. Визначення оцінки адекватності моделі інформаційної безпеки.

Тема 9. Моделювання процесу оцінювання інформаційної безпеки на основі експертних висновків

Рівні інформаційної безпеки. Мультиплікативна згортка інтегрального критерію інформаційної безпеки. Ієрархія елементів інформаційної безпеки управляючих систем.

Тема 10. Функціональна модель системи забезпечення інформаційної безпеки

Статистика порушень інформаційної безпеки. Критерії і умови застосування функціональної моделі. Побудова функціональної моделі системи забезпечення інформаційної безпеки.

Розділ 3. Загрози інформації

Тема 11. Поняття загрози інформації

Визначення поняття «загроза інформації». Формальний опис основних загроз інформації. Класи загроз інформації. Шляхи реалізації загроз інформації.

Тема 12. Загрози порушення конфіденційності інформації

Визначення поняття «конфіденційність інформації». Заходи протидії загрозам конфіденційності інформації. Аналіз прихованих каналів. Забезпечення конфіденційності при обміні.

Тема 13. Загрози порушення цілісності інформації

Визначення поняття «конфіденційність інформації». Заходи протидії загрозам порушення цілісності інформації. Повернення захищеного об'єкту в попередній стан.

Тема 14. Загрози порушення доступності інформації

Визначення поняття «доступність інформації». Працездатність інформаційної системи. Стійкість від відмов. Відновлення після збоїв.

Тема 15. Побудова систем захисту від загроз інформації

Системи захисту від порушення конфіденційності. Системи захисту від порушення цілісності. Системи захисту від порушення доступності.

Тема 16. Моделювання загроз

Метод Делфі. Зовнішні і внутрішні фактори, що впливають на інформацію. Методи оцінки втрат. Стандарт ISO 13335.

3. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб.	інд.	с.р.		л	п	лаб.	інд.	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Розділ 1. Практична методологія IT-аудиту												
Тема 1. Вступ: актуальність IT-аудиту, завдання IT-аудитора	2	2					2	2				
Тема 2. Об’єкти та межі аудиту інформаційних систем	18	2	2			14	18	2	2			14
Тема 3. Заходи контролю інформаційних систем	16	2				14	16	2				14
Тема 4. Критерії IT-аудиту	16	2				14	16	2				14
Тема 5. Інструменти і прийоми комп'ютеризованої підтримки аудиту (CAATTs)	6	2	4				6	2	4			
Разом за розділом 1	**58**	**10**	**6**			**42**	**58**	**10**	**6**			**42**
Розділ 2. Оцінка інформаційної безпеки управляючих систем												
Тема 6. Моделювання інформаційної безпеки	4	2	2					2	2			
Тема 7. Моделі ідентифікації поточного стану інформаційної безпеки	16	2				14	16	2				14
Тема 8. Визначення факторів, які впливають на стан інформаційної безпеки	4	2	2				4	2	2			
Тема 9. Моделювання процесу оцінювання	16	2				14	16	2				14

інформаційної безпеки на основі експертних висновків												
Тема 10. Функціональна модель системи забезпечення інформаційної безпеки	22	2				20	22	2				20
Разом за розділом 2	**62**	**10**	**4**			**48**	**62**	**10**	**4**			**48**
Розділ 3. Загрози інформації												
Тема 11. Поняття загрози інформації	2	2					2	2				
Тема 12. Загрози порушення конфіденційності інформації	16	2				14	16	2				14
Тема 13. Загрози порушення цілісності інформації	4	2	2				4	2	2			
Тема 14. Загрози порушення доступності інформації	16	2				14	16	2				14
Тема 15. Побудова систем захисту від загроз інформації	16	2				14	16	2				14
Тема 16. Моделювання загроз	6	2	4				6	2	4			
Разом за розділом 3	**60**	**12**	**6**			**42**	**60**	**12**	**6**			**42**
Усього годин	**180**	**32**	**16**			**132**	**180**	**32**	**16**			**132**

4. Теми семінарських (практичних, лабораторних) занять

№ з/п	Назва теми	Кількість годин
1.	Рівні аудиту інформаційних систем	2
2.	Постановка проблеми аудиту безпеки інформаційних систем	2
3.	Особливості автоматизованих інформаційних систем як об’єктів ІТ-аудиту	2
4.	Збір інформації для проведення ІТ-аудиту	2
5.	Підготовка рекомендацій та технічної документації з проведення ІТ-аудиту	4

6.	Аналіз результатів IT-аудиту	4
7.	Засоби аналізу та управління ризиками CRAMM	2
Разом		**16**

5. Завдання для самостійної робота

№ з/п	Види, зміст самостійної роботи	Кількість годин
1.	Регламентація аудиту інформаційно-управляючих систем	14
2.	Стан ринку послуг з проведення ІТ-аудиту в Україні	14
3.	Національні та міжнародні стандарти проведення ІТ-аудиту	14
4.	Особливості ІТ-аудит підприємств, які використовують аутсорсинг	14
5.	Протоколи захисту персональних даних та забезпечення інформаційної безпеки в державному секторі	14
6.	Методи оцінки вартості інформаційних ресурсів	14
7.	Спеціальне програмне забезпечення адміністраторів інформаційної безпеки	14
8.	Моделювання доступу до інформаційних систем	14
9.	ІТ-менеджмент. Усвідомлення результатів ІТ-аудиту	20
Разом		**132**

6. Методи навчання

Як правило лекційні та практичні заняття проводяться аудиторно. В умовах дії карантину заняття, відповідно до Наказу ректора Харківського національного університету імені В.Н. Каразіна, проводяться дистанційно за допомогою платформ Google Meet та Google Classroom.

7. Методи контролю

Контроль роботи студентів при вивченні дисципліни і засвоєння ними навчального матеріалу здійснюється на практичному зайнятті шляхом проведення «летючок», контрольних опитувань і захисту звітів з практичних домашніх завдань. Підсумковий контроль здійснюється на екзамені.

Студенти, що не захистили впродовж семестру звіти з практичних завдань, до екзамену не допускаються.

Екзаменаційний квиток містить два теоретичних і одне практичне питання. Максимальна кількість балів за відповіді на кожне теоретичне питання складає по 12 балів, на практичне питання – 16 балів.

8. Схема нарахування балів

Розподіл балів для підсумкового семестрового контролю при проведенні екзаменаційної роботи

Поточний контроль						Разом	Екзаменаційна робота	Сума
Розділ 1		Розділ 2		Розділ 3				
Т2	Т5	Т6	Т8	Т13	Т16	60	40	100
10	10	10	10	10	10			

Загальні критерії оцінювання

№	Форми навчальної діяльності	Кількість балів	Термін	Примітки
1.	Виконання практичних робіт	10	постійно	
2.	Екзаменаційна робота	40	грудень	
Всього		**100**		

Критерії оцінювання знать студентів під час поточного контролю

Кожна практична робота оцінюється від 0 до 10 балів:

8-10 балів: студент самостійно виконав практичну роботу, розуміє зміст роботи, може дати відповіді на запитання щодо виконаної роботи, вільно орієнтується в програмній реалізації, може вносити в програмну реалізацію незначні зміни;

6-7 балів: студент виконав практичну роботу, має розуміння щодо її змісту, орієнтується в програмній реалізації, але не може дати вільно відповідь на додаткові питання або внести зміни до програмній реалізації, потребує для цього часу та додаткових матеріалів;

4-5 балів: студент виконав практичну роботу, але має погане розуміння щодо її змісту, майже не орієнтується в програмній реалізації;

1-3 бали: студент виконав практичну роботу, але не має жодного розуміння щодо її змісту, не орієнтується в програмній реалізації;

0 балів: студент не виконав практичну роботу.

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка	
	для чотирирівневої шкали оцінювання	для дворівневої шкали оцінювання
90-100	відмінно	зараховано
70-89	добре	
50-69	задовільно	
1-49	незадовільно	не зараховано

9. Рекомендована література

Основна література

1. Антонюк А.О. Моделювання систем захисту інформації: Монографія. – Ірпінь: Національний університет ДПС України, 2015. – 273 с.

2. Гаврилова Л.В. Практична методологія ІТ-аудиту. – К.: Наукова думка, 2015. – 304 с.

3. Ус Р.Л. Моделі аудиту інформаційних технологій. – К.: Фенікс, 2013. – 146 с.

4. Міжнародні стандарти контролю якості аудиту: 2-е вид., пер. з англ. Біндера К.С. – К.: Новий формат, 2016. – 613 с.

5. Гузик С.С. Управління та аудит інформаційних технологій. – К.: Jet Info, 2009 – 263 с.

6. Славкова О.П. Особливості проведення аудиту в інформаційному середовищі. – Харків: Ранок, 2011. – 351 с.

7. Значення ІТ-аудиту та його перспективи в Україні: Монографія. – Львів: Видавництво Лева, 2012. – 286 с.

Допоміжна література

1. Родіонов А.М. Логіко-імовірнісна модель захищеності компонентів інформаційно-комунікаційних систем / Родіонов А.М., Новіков О.М. // Інформаційні технології та комп`ютерна інженерія. – 2008. – № 1 (11). – С. 170- 175.

2. НД ТЗІ. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–002–99. – Київ: ДСТСЗІ СБ України, 1999. – 16 с.

3. НД ТЗІ. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2–004–99. – Київ: ДСТСЗІ 497 СБ України, 1999. – 55 с.

4. НД ТЗІ. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.2–005–99. – Київ: ДСТСЗІ СБ України, 1999. – 23 с.

5. НД ТЗІ. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99. – Київ: ДСТСЗІ СБ України, 1999. – 26 с.

6. Жора В.В. Аспекти застосування теорії функціонування організаційних систем до вирішення задач керування захистом інформації, – Київ: 2007, №14.

7. Глушков В.М. Основы безбумажной информатики. – М.: Наука, 1978. – 552 с.

8. Chunxiao Y., Zhongfu W., and Yunqing F. An Attribute-Based Delegation Model and Its Extension // J. Res. Practice Inform. Technol. 2006. V. 38. No. 1. P. 220-234.

9. McLean J., John D. A Comment on the «Basic Security Theorem» of Bell and LaPadula // Information Processing Letters.-1985.-Vol. 20, № 2, Feb.

10. Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

1. http://en.wikipedia.org/wiki/Information_technology_audit
2. https://audit.gov.ua/
3. http://active-solutions.com.ua/uk/
4. https://www.easy-tech.ru/articles/it_audit_glavnye_tseli_i_osnovnye_etapy/
5. https://www.isaca.org/bookstore/audit-control-and-security-essentials/witaf
6. https://study.com/academy/lesson/isaca-it-audit-standards-tools-phases.html
7. https://www.academia.edu/11355605/Auditing_Standards_for_auditing_Information_Systems?auto=download

Додаток 1

Додаток до робочої програми навчальної дисципліни **«Моніторинг та аудит інформаційно-управляючих систем»**

Дію робочої програми продовжено: на 20___/20___ н. р.

Заступник декана факультету комп’ютерних наук з навчальної роботи

_____ Є.П. КОЛОВАНОВА

«____» _____ 20___ р.

Голова методичної комісії факультету комп’ютерних наук

_____ А.Г. БЄРДНІКОВ

«____» _____ 20___ р.