Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра теоретичної та прикладної системотехніки

"ЗАТВЕРДЖУЮ"

Проректор з науково-педагогічної роботи

_____

"____"_____2019 р.

Робоча програма навчальної дисципліни

Моніторинг та аудит інформаційно-управляючих систем

рівень вищої освіти другий (магістерський)

спеціальність 123 «Комп'ютерна інженерія»

освітня програма Комп'ютерна інженерія

вид дисципліни за вибором

факультет комп'ютерних наук

2019 / 2020 навчальний рік

Програму обговорено та рекомендовано до затвердження вченою радою факультету комп'ютерних наук
«28» серпня2019 р., протокол № 3

РОЗРОБНИК ПРОГРАМИ:

кандидат економічних наук, доцент кафедри теоретичної та прикладної системотехніки **Чуб Ольга Ігорівна.**

Програму схвалено на засіданні кафедри теоретичної та прикладної системотехніки
Протокол від " 19 " червня 2019 року № 14

Завідувач кафедри теоретичної та прикладної системотехніки
_____ Шматков С. І.

Програму погоджено методичною комісією факультету комп'ютерних наук
Протокол від " 20 " червня 2019 року № 9

Голова методичної комісії факультету комп'ютерних наук
_____ Бердніков А. Г.

ВСТУП

Програма навчальної дисципліни «Моніторинг та аудит інформаційно-управляючих систем» розроблена відповідно до освітньо-професійної програми підготовки другого (магістерського) рівня спеціальності 123 «Комп'ютерна інженерія».

1. Опис навчальної дисципліни

1.1. Мета викладання навчальної дисципліни.

Метою викладання дисципліни 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.

Викладання дисципліни передбачає поєднання фундаментальної підготовки в області інформаційних технологій з вивченням методик і спеціалізованих програмних продуктів аудиту інформаційних систем.

Об'єктом вивчення дисципліни є – моделі безпеки інформації, а також пов'язані з ними методи проведення аудиту інформаційно-управляючих систем та дослідження процесу захисту інформації; методи й алгоритми оцінки ефективності проведених аудиторських процедур, методи ідентифікації загроз в задачах моніторингу і прогнозування стану інформаційної безпеки.

Предметом вивчення дисципліни є – стан організаційних, інформаційних та інших характеристик комп'ютерних систем, які знаходяться в сфері аудиторської оцінки рівня безпеки.

1.2. Завдання навчальної дисципліни.

Завданнями навчальної дисципліни є вивчення:

– 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.

1.3. Кількість кредитів – 6.

1.4. Загальна кількість годин – 180.

1.5. Характеристика навчальної дисципліни	
За вибором	
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.
Індивідуальні завдання	
0 год.	

1.6. Заплановані результати навчання

Відповідно до вимог освітньо-кваліфікаційного рівня підготовки за результатами вивчення дисципліни студенти повинні –

знати:

- основні поняття аудиту інформаційних систем та інформаційної безпеки;
- методи аналізу та оцінки захищеності автоматизованих інформаційних систем;
- національні та міжнародні стандарти в галузі проведення ІТ-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 ІТ-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 ІТ-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.

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				
Тема 2. Об’єкти та межі аудиту інформаційних систем		2	2			14		2	2			14
Тема 3. Заходи контролю інформаційних систем		2				14		2				14
Тема 4. Критерії IT-аудиту		2				14		2				14
Тема 5. Інструменти і прийоми комп'ютеризованої підтримки аудиту (CAATTs)		2	4					2	4			
Разом за розділом 1		10	6			42		10	6			42
Розділ 2. Оцінка інформаційної безпеки управляючих систем												
Тема 6. Моделювання інформаційної безпеки		2	2					2	2			
Тема 7. Моделі ідентифікації поточного стану інформаційної безпеки		2				14						14
Тема 8. Визначення факторів, які впливають на стан інформаційної безпеки		2	2					2	2			
Тема 9. Моделювання процесу оцінювання інформаційної безпеки на основі експертних висновків		2				14		2				14

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

4. Теми практичних занять

№ п/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 ІТ-аудиту	4
7	Засоби аналізу та управління ризиками CRAMM	2
	Разом	16

5. Завдання для самостійної роботи

№ п/п	Зміст	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-менеджемент. Усвідомлення результатів ІТ-аудиту	20
	Разом	132

6. Індивідуальні завдання

Індивідуальне завдання пов'язане із застосуванням на практиці методології проведення ІТ-аудиту та підготовкою технічної документації за його результатами.

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

Поточний контроль																	
Розділ 1					Розділ 2						Розділ 3						Сума балів
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т8	Т9	Т10	Т11	Т12	Т13	Т14	Т15	Т16	
2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	50

Самостійна робота, індивідуальні завдання			**Загальна сума балів**
Контрольна робота	Індивідуальне завдання	Екзамен	
-	10	40	**100**

Критерії оцінювання знань студентів за практичні роботи

Вимоги	Кількість балів
.▪ Завдання відзначається повнотою виконання без допомоги викладача. ▪ Визначає рівень поінформованості, потрібний для прийняття рішень. Вибирає інформаційні джерела,. ▪ Робить висновки і приймає рішення у ситуації невизначеності. Володіє уміннями творчо-пошукової діяльності.	5
▪ Завдання – повні, з деякими огріхами, виконані без допомоги викладача. ▪ Планує інформаційний пошук; володіє способами систематизації інформації; ▪ Робить висновки і приймає рішення у ситуації невизначеності. Володіє уміннями творчо-пошукової діяльності.	4
▪ Завдання відзначається неповнотою виконання без допомоги викладача. ▪ Студент може зіставити, узагальнити, систематизувати інформацію під керівництвом викладача; вільно застосовує вивчений матеріал у стандартних ситуаціях.	3
▪ Завдання відзначається неповнотою виконання за консультацією викладача. ▪ Застосовує запропонований вчителем спосіб отримання інформації, має фрагментарні навички в роботі з підручником, науковими джерелами; ▪ Вибирає відомі способи дій для виконання фахових методичних завдань.	2
Завдання відзначається фрагментарністю виконання за консультацією викладача або під його керівництвом.	1

Критерії оцінювання знань студентів за контрольну роботу

Вимоги	Кількість балів
Повнота виконання завдання повна, студент здатен формулювати закони та закономірності, структурувати судження, умовиводи, доводи, описи.	8-10
Повнота виконання завдання повна, студент здатен формулювати операції, правила, алгоритми, правила визначення понять.	5-7
Повнота виконання завдання елементарна, студент здатен вибирати відомі способи дій для виконання фахових завдань.	3-5
Повнота виконання завдання фрагментарна.	1-2

Критерії оцінювання залікових робіт студентів

Вимоги	Кількість балів
Показані всебічні систематичні знання та розуміння навчального матеріалу; безпомилково виконані завдання.	35-40

Показані повні знання навчального матеріалу; помилки, якщо вони є, не носять принципового характеру.	30-35
Показано повне знання необхідного навчального матеріалу, але допущені помилки.	20-30
Показано повне знання необхідного навчального матеріалу, але допущені суттєві помилки	10-20
Показано недосконале знання навчального матеріалу, допущені суттєві помилки.	5-10
Показано недосконале знання навчального матеріалу, допущені суттєві помилки, які носять принциповий характер; обсяг знань не дозволяє засвоїти предмет.	1-5

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 IT-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 IT-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 / Новіков О.М., Родіонов А.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