Харківський національний університет імені В.Н. Каразіна
Факультет комп'ютерних наук
Кафедра теоретичної та прикладної системотехніки

УХВАЛЕНО
Вченою радою факультету
комп'ютерних наук, протокол № 4
від «03» грудня 2019 р.
Голова Вченої ради _____

Назва курсу	Моніторинг та аудит інформаційно-управляючих систем
Викладачі	Чуб Ольга Ігорівна
Профайли викладачів	https://scholar.google.com.ua/citations?user=eCM1V6UAAAAJ&hl=uk
Контактний телефон	+38(067)581-45-64 Чуб Ольга Ігорівна
E-mail:	o.i.chub@karazin.ua Чуб Ольга Ігорівна
Сторінка курсу в системі дистанційного навчання	
Консультації	*Очні консультації* Чуб Ольга Ігорівна: кожен вівторок з 12.30 до 13.30 в ауд. 319 північного корпусу

1. Коротка анотація до курсу

Програма курс «Моніторинг та аудит інформаційно-управляючих систем» розроблена відповідно до освітньо-професійної програми підготовки студентів спеціальності 123 «Комп'ютерна інженерія».

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.

2. Мета та цілі курсу

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.

Ціллю курсу 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.

3. Формат курсу – дистанційний.

4. Результати навчання

Після вивчення курсу студент:

знає:

- 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;
- основи контролю процесів в інформаційних системах;

уміє:

- 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.

5. Обсяг курсу

Вид заняття	Загальна кількість годин
лекції	32
семінарські заняття / практичні / лабораторні	16
самостійна робота	132

6. Ознаки курсу:

Рік викладання	Семестр	Спеціальність	Курс (рік навчання)	Нормативний\ вибірковий
2020	1	123 «Комп'ютерна інженерія»	1	вибірковий

7. Пререквізити

Дисциплінами, що передують курсу «Моніторинг та аудит інформаційно-управляючих систем» є такі: «Технології захисту інформації», «Теорія інтелектуальних систем та аналіз даних», «Захист інформації в інформаційно-комунікаційних системах», «Комп'ютерні системи прийняття рівень».

Студент, щоб приступити до вивчення дисципліни «Моніторинг та аудит інформаційно-управляючих систем», повинен знати: визначення понять теорії матриць і визначників; методи розв'язання систем лінійних рівнянь; поняття та теореми диференціального і інтегрального числення. Крім того, студент повинен вміти розв'язувати приладні задачі за допомогою надбудови «Пошук рішення» в пакеті MS Excel та використовувати технологію об'єктно-орієнтованого програмування для побудови моделей та розв'язання оптимізаційних задач.

8. Технічне та програмне забезпечення /обладнання

Для вивчення матеріалу курсу студенту необхідно буде працювати з пакетами MS Excel, середовищем розробки з підтримкою мови програмування Python або іншої мови об'єктно-орієнтованої мови програмування (за вибором студента).

9. Політики курсу

Під час вивчення курсу «Моніторинг та аудит інформаційно-управляючих систем» необхідно дотримуватися усіх етичних принципів та норм академічної доброчесності, визначених Листом Міністерства освіти і науки України № 1/-650 від 23.11.2018 року «Щодо рекомендацій з академічної доброчесності для закладів вищої освіти», а саме:

- самостійно виконувати навчальні завдання, завдання поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);

- здійснювати посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;

- дотримуватися норм законодавства про авторське право і суміжні права;

- надавати достовірну інформацію про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

10. Схема курсу

Тиждень / дата / кількість академічних годин	Тема, план, короткі тези	Форма заняття / формат заняття	Матеріали	Література / Електронні ресурси	Завдання, кількість год	Вага оцінки	Термін виконання
Тиждень № 1 / вересень 2020 р. / 2 академічні години	**Тема № 1** «Вступ: актуальність IT-аудиту, завдання IT-аудитора»: - Передумови виникнення та етапи розвитку концепції IT-аудиту. IT-аудит як ключовий компонент забезпечення якості інформаційних систем. Узагальнена класифікація видів IT-аудитів. Нормативно-правове забезпечення IT-аудиту. Термінологія та основні поняття IT-аудиту.	Лекція / дистанційна	Презентація лекції	[1-6]	Ознайомитись з літературою, переглянути презентацію, 2 години	2	Протягом тижня (до наступної лекції)

Тиждень № 2 / вересень 2020 р. / 2 академічні години	**Тема № 2** «Об'єкти та межі аудиту інформаційних систем»: - типові фактори ризику в аудиті інформаційних систем; - аспекти якості IT-аудиту; - рівні IT-аудиту; - результативність структури та операційні результативність заходів аудиту та моніторингу інформаційних систем; - IT-аудит в державних установах.	Лекція / дистанційна	Презентація лекції	[1-6]	Ознайомитись з літературою, переглянути презентацію, 2 години	3	Протягом тижня (до наступної лекції)
Тиждень № 2 / вересень 2020 р. / 2 академічні години	**Тема № 1** «Рівні аудиту інформаційних систем»	Практична робота / дистанційна	Методичні вказівки до виконання лабораторних робіт	[1-6, 9-10]	Проаналізувати та ранжувати за рівнями типи аудиту інформаційної системи відповідно до варіанту, підготувати письмовий звіт, 2 години	5	Протягом тижня (до наступної практичної роботи)

Тиждень № 3 / вересень 2020 р. / 2 академічні години	**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.	Лекція / дистанційна	Презентація лекції	[1-10]	Ознайомитись з літературою, переглянути презентацію, 2 години	3	Протягом тижня (до наступної лекції)
Тиждень № 4 / вересень 2020 р. / 2 академічні години	**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).	Лекція / дистанційна	Презентація лекції	[1-10]	Ознайомитись з літературою, переглянути презентацію, 2 години	3	Протягом тижня (до наступної лекції)

Тиждень № 5 / жовтень 2020 р. / 2 академічні години	**Тема № 5** «Інструменти і прийоми комп'ютеризованої підтримки аудиту (CAATTs»: - інструменти: NMAP, OWASP ZAP, Splunk, Flexicon Disco, Qlikview; - приклади використання інструментів IT-аудиту.	Лекція / дистанційна	Презентація лекції	[7-12]	Ознайомитись з літературою, переглянути презентацію, 2 години	3	Протягом тижня (до наступної лекції)
Тиждень № 5 / жовтень 2020 р. / 2 академічні години	**Тема № 1** «Постановка проблеми аудиту безпеки інформаційних систем»	Практична робота / дистанційна	Методичні вказівки до виконання лабораторних робіт	[1-6, 9-10]	Сформулювати та математично записати поставку проблеми аудиту безпеки інформаційної системи відповідно до варіанту, надати рекомендації з розв’язання проблеми, підготувати письмовий звіт, 2 години	5	Протягом тижня (до наступної практичної роботи)

Тиждень № 6 / жовтень 2020 р. / 2 академічні години	**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).	Лекція / дистанційна	Презентація лекції	[5-13]	Ознайомитись з літературою, переглянути презентацію, 2 години	3	Протягом тижня (до наступної лекції)
Тиждень № 6 / жовтень 2020 р. / 2 академічні години	**Тема № 1** «Особливості автоматизованих інформаційних систем як об'єктів IT-аудиту»	Практична робота / дистанційна	Методичні вказівки до виконання лабораторних робіт	[1-6, 9-10]	Виділити та описати особливості інформаційної системи відповідно до варіанту, підготувати письмовий звіт, 2 години	5	Протягом тижня (до наступної практичної роботи)
Тиждень № 7 / жовтень 2020 р. / 2 академічні години	**Тема № 7** «Моделі ідентифікації поточного стану інформаційної безпеки»: - модель Threat and Risk Assessment (TRA)	Лекція / дистанційна	Презентація лекції	[5-14]	Ознайомитись з літературою, переглянути презентацію, 2 години	3	Протягом тижня (до наступної лекції)

Тиждень № 8 / жовтень 2020 р. / 2 академічні години	**Тема № 8** «Визначення факторів, які впливають на стан інформаційної безпеки»: - методи визначення ступеню взаємозв'язків між факторами та їх влив на стан безпеки; - визначення оцінки адекватності моделі інформаційної безпеки.	Лекція / дистанційна	Презентація лекції	[5-14]	Ознайомитись з літературою, переглянути презентацію, 2 години	3	Протягом тижня (до наступної лекції)
Тиждень № 8 / жовтень 2020 р. / 2 академічні години	**Тема № 1** «Збір інформації для проведення аудиту»	Практична робота / дистанційна	Методичні вказівки до виконання лабораторних робіт	[1-6, 9-10]	Провести детальний аналіз інформаційної системи відповідно до варіанту, знайти та описати слабкі місця в системі, підготувати письмовий звіт, 2 години	5	Протягом тижня (до наступної практичної роботи)
Тиждень № 9 / жовтень 2020 р. / 2 академічні години	**Тема № 9** «Моделювання процесу оцінювання інформаційної безпеки на основі експертних висновків»: - рівні інформаційної безпеки;	Лекція / дистанційна	Презентація лекції	[5-14]	Ознайомитись з літературою, переглянути презентацію, 2 години	3	Протягом тижня (до наступної лекції)

	- мультиплікативна згортка інтегрального критерію інформаційної безпеки; - ієрархія елементів інформаційної безпеки управляючих систем.						
Тиждень № 10 / листопад 2020 р. / 2 академічні години	**Тема № 10** «Функціональна модель системи забезпечення інформаційної безпеки»: - критерії і умови застосування функціональної моделі; - побудова функціональної моделі системи забезпечення інформаційної безпеки.	Лекція / дистанційна	Презентація лекції	[1-2, 7-14]	Ознайомитись з літературою, переглянути презентацію, 2 години	3	Протягом тижня (до наступної лекції)
Тиждень № 11 / листопад 2020 р. / 2 академічні години	**Тема № 11** «Поняття загрози інформації»: - Визначення поняття «загроза інформації»; - формальний опис основних загроз інформації; - класи загроз інформації; - шляхи реалізації загроз інформації.	Лекція / дистанційна	Презентація лекції	[1-7, 9-14]	Ознайомитись з літературою, переглянути презентацію, 2 години	3	Протягом тижня (до наступної лекції)

Тиждень № 12 / листопад 2020 р. / 2 академічні години	**Тема № 12** «Загрози порушення конфіденційності інформації»: - визначення поняття «конфіденційність інформації»; - заходи протидії загрозам конфіденційності інформації; - аналіз прихованих каналів; - забезпечення конфіденційності при обміні.	Лекція / дистанційна	Презентація лекції	[5-7, 9-14]	Ознайомитись з літературою, переглянути презентацію, 2 години	3	Протягом тижня (до наступної лекції)
Тиждень № 13 / листопад 2020 р. / 2 академічні години	**Тема № 13** «Загрози порушення цілісності інформації»: - визначення поняття «конфіденційність інформації»; - заходи протидії загрозам порушення цілісності інформації; - повернення захищеного об’єкту в попередній стан.	Лекція / дистанційна	Презентація лекції	[1, 5-7, 9-14]	Ознайомитись з літературою, переглянути презентацію, 2 години	3	Протягом тижня (до наступної лекції)

Тиждень № 13 / грудень 2020 р. / 4 академічні години	**Тема № 1** «Підготовка рекомендацій та технічної документації з проведення IT-аудиту»	Практична робота / дистанційна	Методичні вказівки до виконання лабораторних робіт	[1-6, 9-10]	Провести IT-аудит інформаційної системи відповідно до варіанту, заповнити відповідну технічну документацію, підготувати письмовий звіт, 4 години	5	Протягом тижня (до наступної практичної роботи)
Тиждень № 14 / грудень 2020 р. / 2 академічні години	**Тема № 14** «Загрози порушення доступності інформації»: - визначення поняття «доступність інформації»; - працездатність інформаційної системи.	Лекція / дистанційна	Презентація лекції	[9-15]	Ознайомитись з літературою, переглянути презентацію, 2 години	3	Протягом тижня (до наступної лекції)
Тиждень № 15 / грудень 2020 р. / 2 академічні години	**Тема № 15** «Побудова систем захисту від загроз інформації»: - системи захисту від порушення конфіденційності; - системи захисту від порушення цілісності; - системи захисту від порушення доступності.	Лекція / дистанційна	Презентація лекції	[6, 9-14]	Ознайомитись з літературою, переглянути презентацію, 2 години	3	Протягом тижня (до наступної лекції)

Тиждень № 15 / грудень 2020 р. / 4 академічні години	**Тема № 1** «Аналіз результатів IT-аудиту»	Практична робота / дистанційна	Методичні вказівки до виконання лабораторних робіт	[1-6, 9-10]	Розглянути технічну документацію IT-аудиту інформаційної системи відповідно до варіанту, підготувати комплекс рекомендації з підвищення рівня безпеки, підготувати письмовий звіт, 4 години	5	Протягом тижня (до наступної практичної роботи)
Тиждень № 16 / грудень 2020 р. / 2 академічні години	**Тема № 16** «Моделювання загроз»: - метод Делфі; - зовнішні і внутрішні фактори, що впливають на інформацію; - методи оцінки втрат; - стандарт ISO 13335.	Лекція / дистанційна	Презентація лекції	[6, 9-16]	Ознайомитись з літературою, переглянути презентацію, 2 години	3	*Заключна лекція*. Вивчити матеріал до заключного практичного заняття

11. Система оцінювання та вимоги

Загальна система оцінювання курсу	Впродовж семестру студент набирає до *100* балів. До *60* балів – за виконання практичних робіт. До *40* балів – під час складання іспиту.
Вимоги до письмової роботи	На кожне практичне заняття студент повинен підготувати письмовий звіт про виконання відповідної практичної роботи. В звіті наводиться коротка теоретична довідка про матеріал, який вивчався на практичному занятті, описується порядок виконання завдання в залежності від варіанту, виконується детальний аналіз отриманих результатів. Кількість сторінок звіту – від 4 до 6. Звіт здається у роздрукованій формі.
Семінарські заняття	В курсі «Моніторинг та аудит інформаційно-управляючих систем» не заплановані семінарські заняття.
Умови допуску до підсумкового контролю	Студент отримає допуск до екзамену після успішної здачі та захисту звітів з виконання усіх практичних робіт.

12. Рекомендована 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, доп.., 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. Жора В.В. Аспекти застосування теорії функціонування організаційних систем до вирішення задач керування захистом інформації, – Київ: 2007, №14.
14. Глушков В.М. Основы безбумажной информатики. – М.: Наука, 1978. – 552 с.
15. 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.
16. McLean J., John D. A Comment on the «Basic Security Theorem» of Bell and LaPadula // Information Processing Letters.-1985.-Vol. 20, № 2, Feb.