Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та математики

Кафедра інформаційної та кібернетичної безпеки

імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«___» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «МОНІТОРИНГ, АУДИТ ТА АДМІНІСТРУВАННЯ ЗАХИЩЕНИХ ІТ СИСТЕМ І МЕРЕЖ»

для студентів

спеціальності	125 Кібербезпека та захист інформації
освітнього рівня	другого (магістерського)
освітньої програми	125.00.02 Безпека інформаційних і комунікаційних систем

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 0125/23
(підпис) (прізвище, ініціали)
«___» _____ 2023 р.

2023 – 2024 навчальний рік

Розробник:

Аносов Андрій Олександрович, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Аносов Андрій Олександрович, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 01.09.2022 р. № 12

Завідувач кафедри _____ (підпис) Павло СКЛАДАННИЙ

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.02 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.

Керівник освітньої програми ___ (підпис) Володимир СОКОЛОВ

Робочу програму перевірено

___.___. 2022 р.

Заступник декана _____ (підпис) Євген ІВАНІЧЕНКО

Пролонговано:

на 2023/2024 н.р. _____ (_____), «23» 08 2023 р., протокол № 8
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання		
	денна		заочна
Вид дисципліни	вибіркова		
Мова викладання, навчання та оцінювання	українська		
Загальний обсяг кредитів / годин	7 / 210		
Курс	1		
Семестр	1	2	
Кількість змістових модулів з розподілом:	3		
Обсяг кредитів	5	2	
Обсяг годин, в тому числі:	120	90	
Аудиторні	32	24	
Модульний контроль	8	4	
Семестровий контроль	-	30	
Самостійна робота	80	32	
Форма семестрового контролю	залік	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Моніторинг, аудит та адміністрування захищених ІТ систем і мереж» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів другого (магістерського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека та захист інформації, освітньої програми 125.00.02 Безпека інформаційних і комунікаційних систем.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач другого (магістерського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Моніторинг, аудит та адміністрування захищених ІТ систем і мереж» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Моніторинг, аудит та адміністрування захищених ІТ систем і мереж» складається з трьох змістових модулів: Моніторинг захищених ІТ систем і мереж. Основи застосування DLP-систем; Адміністрування захищених ІТ систем і мереж; Аудит захищених ІТ систем і мереж. Обсяг дисципліни – 210 год. (7 кредитів).

Метою викладання навчальної дисципліни «Моніторинг, аудит та адміністрування захищених ІТ систем і мереж» є формування у студентів уміння вирішувати задачі адміністрування захищених інформаційно-телекомунікаційних систем, застосовувати нормативно-правові, організаційні та технічні процедури моніторингу та аудиту захищених інформаційно-телекомунікаційних систем.

Завдання полягає у формуванні теоретичних знань та практичних умінь у сфері інформаційної та кібернетичної безпеки та набуття **наступних фахових компетентностей**:

ФК 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.

ФК 5: 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.

ФК 6: Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або

кібербезпеки організації.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен

знати:

- основні завдання, функції, обов'язки та права адміністратора безпеки щодо аналізу, контролю та забезпеченню системи управління доступом до інформаційних ресурсів згідно встановленої політики інформаційної безпеки;
- основи експлуатації захищених інформаційно-комунікаційних систем;
- експлуатаційно-технічні характеристики оцінювання ступеня працездатності інформаційно-комунікаційних систем;
- завдання технічного персоналу із забезпечення інформаційної безпеки інформаційно-комунікаційних систем;
- порядок розробки, реалізації та супроводження проектів з захисту інформації;
- методики моніторингу та аудиту захищених інформаційно-комунікаційних систем, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації;
- цілі та основні методики проведення аудиту ІТ систем і мереж;
- види та місцезнаходження інформації, яка може бути виявлена під час проведення аудиту;
- етапи та послідовність проведення моніторингу та аудиту ІТ систем і мереж;
- методики та програмні засоби, за допомогою яких може біти проведених моніторинг та аудит у певної інформаційної системі.

уміти:

- планувати та проводити заходи захисту в умовах експлуатації комп’ютерних систем та мереж;
- розробляти та впроваджувати політику безпеки комп’ютерних систем та мереж;
- аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до політики інформаційної безпеки організації;
- здійснювати експлуатаційні заходи захисту інформації комп’ютерної мережі (системи) та на підсистемах;
- обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту;
- розробляти, реалізовувати та супроводжувати проекти з захисту інформації;
- аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій;
- характеризувати основні етапи проведення аудиту безпеки захищених комп’ютерних систем та мереж;
- проводити моніторинг ІТ систем і мереж із використанням сучасних методик та програмних засобів;
- самостійно обробити дані, що були отримані під час моніторингу ІС;
- визначати основні вразливості, які були виявлені під час моніторингу інформаційної системи;
- надавати рекомендації по усуненню виявлених уразливостей безпеки ІС.

та досягти наступних **програмних результатів навчання:**

РН 11: Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН 14: 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.

РН 19: Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту
інтелектуальної власності.

РН(У) 24: Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях та SMART -інфраструктурі. Вміти проектувати захищені (з урахуванням загроз) проводові і безпроводові телекомунікаційні та SMART -системи.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
СЕМЕСТР 1							
Змістовий модуль 1. Моніторинг захищених ІТ систем і мереж. Основи застосування DLP-систем							
Тема 1. Моніторинг захищених ІТ систем і мереж та системи безпеки.	56	6		4	6		40
Модульний контроль	4						
Разом	60	6		4	6		40
Змістовий модуль 2. Адміністрування захищених ІТ систем і мереж							
Тема 2. Адміністрування інформаційних систем і політика безпеки.	56	6		6	4		40
Модульний контроль	4						
Разом	60	6		6	4		40
Усього за семестр 1	**120**	**12**		**10**	**10**		**80**
СЕМЕСТР 2							
Змістовий модуль 3. Аудит захищених ІТ систем і мереж							
Тема 3. Аудит захищених ІТ систем і мереж та системи безпеки.	56	8		8	8		32
Модульний контроль	4						
Разом	60	8		8	8		32
Підготовка та проходження контрольних заходів	30						
Усього за семестр 2	**90**	**8**		**8**	**8**		**32**
Усього	**210**	**20**		**18**	**18**		**112**

5. Програма навчальної дисципліни

Змістовий модуль 1. Моніторинг захищених ІТ систем і мереж. Основи застосування DLP-систем

Основні питання:

- Моніторинг захищених ІТ систем і мереж
- Моніторинг безпеки інформаційної системи
- Моніторинг стану ІТ систем і мереж з використанням сканерів безпеки
- Системи запобігання витоку інформації

- Моніторинг поточного функціонування ІТ систем і мереж
- Реалізація оперативного контролю за діями користувачів

Змістовий модуль 2. Адміністрування захищених ІТ систем і мереж

Основні питання:

- Адміністрування інформаційних систем і політика безпеки ІТС
- Захист інформації в комп'ютерних мережах, функції адміністратора безпеки
- Заходи щодо адміністрування базових інформаційних служб
- Адміністрування за допомогою вбудованих та програмних засобів
- Системи виявлення вторгнень
- Побудова захищених мереж відповідно до моделі взаємодії відкритих систем
- Налаштування програмного комплексу SearchInform для контролю мережі

Змістовий модуль 3. Аудит захищених ІТ систем і мереж

Основні питання:

- Основні підходи до реалізації моніторингу та аудиту безпеки інформації
- Заходи щодо аудиту захищених ІТ- систем
- Моніторинг стану ІТ систем і мереж з використанням сканерів безпеки
- Дослідження засобів перешкоджання аудиту інформації в ІТ системі
- Моніторинг поточного функціонування ІТ систем і мереж
- Аудит цілісності файлових систем

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, залік.
- *Комп'ютерного контролю:* програми - емулятори.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види

контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю у 1-му семестрі

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	3	3	3	3
Відвідування семінарських занять	1				
Відвідування практичних занять	1	2	2	3	3
Відвідування лабораторних занять	1	3	3	2	2
Робота на семінарському занятті	10				
Робота на практичному занятті	10	2	20	3	30
Лабораторна робота (в тому числі допуск, виконання, захист)	10	3	30	2	20
Виконання завдань для самостійної роботи	5	3	15	3	15
Виконання модульної роботи	25	1	25	1	25
Виконання ІНДЗ	30				
	Разом	-	98	-	98
Максимальна кількість балів: 196					
Розрахунок коефіцієнта: 196/100=1,96					

Розрахунок рейтингових балів за видами поточного (модульного) контролю у 2-му семестрі

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 3	
		кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	4	4
Відвідування семінарських занять	1		
Відвідування практичних занять	1	4	4
Відвідування лабораторних занять	1	4	4
Робота на семінарському занятті	10		
Робота на практичному занятті	10	4	40
Лабораторна робота (в тому числі допуск, виконання, захист)	10	4	40
Виконання завдань для самостійної роботи	5	4	20
Виконання модульної роботи	25	1	25
Виконання ІНДЗ	30		
	Разом	-	137
Максимальна кількість балів: 137			
Розрахунок коефіцієнта: 137/60=2,28			

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Моніторинг захищених ІТ систем і мереж. Основи застосування DLP-систем		40	15
1	Тема 1. Моніторинг захищених ІТ систем і мереж та системи безпеки.	40	15
	Лекція 1. Моніторинг захищених ІТ систем і мереж: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	13	5
	Лекція 2. Моніторинг безпеки інформаційної системи: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	14	5
	Лекція 3. Виявлення мережевих атак шляхом аналізу трафіка: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	13	5
Змістовий модуль 2. Адміністрування захищених ІТ систем і мереж.		40	15
3	Тема 2. Адміністрування інформаційних систем і політика безпеки.	40	15
	Лекція 1. Адміністрування інформаційних систем і політика безпеки ІТС: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	13	5
	Лекція 2. Захист інформації в комп'ютерних мережах, функції адміністратора безпеки: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	14	5
	Лекція 3. Системи запобігання витоку інформації та виявлення вторгнень: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	13	5
Змістовий модуль 3. Аудит захищених ІТ систем і мереж.		32	20
5	Тема 3. Аудит захищених ІТ систем і мереж та системи безпеки.	32	20
	Лекція 1. Основні підходи до реалізації аудиту безпеки інформації: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	8	5
	Лекція 2. Аудит уразливості захищених інформаційно-комунікаційних систем: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	8	5
	Лекція 3. Аудит інформаційної безпеки із застосуванням методів кластерного аналізу: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	8	5
	Лекція 4. Заходи щодо аудиту захищених ІТ- систем: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	8	5
	Разом	112	50

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – тест, що складається 3 комплексних запитань.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання у 1-му семестрі здійснюється у формі заліку, умовою отримання якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Семестрове (підсумкове) оцінювання у 2-му семестрі здійснюється у формі екзамену, умовою допуску до якого є отриманням студентом 35 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Форма проведення екзамену – комбінована. Іспит оцінюється у 40 балів за розподілом: 20 балів – комплексний тест з дисципліни; 20 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями з побудови інформаційних мереж та управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

Оцінювання практичного завдання відбувається в межах від 0 до 20 балів, згідно критеріїв оцінювання, й здійснюється з урахуванням: рівнів сформованості аналітико-синтетичних, творчих та методичних умінь необхідних для побудови захищених інформаційних та інформаційно-телекомунікаційних (автоматизованих) систем.

Бали за виконання тесту та бали за виконання практичного завдання додаються. Оцінювання результатів засвоєння теоретичних знань та оцінювання сформованості практичних навичок володіння цифровими технологіями студентами, продемонстровані на екзамені, представлене у таблиці.

Підсумкова кількість балів (max – 40)	Оцінка за 4-бальною шкалою
1 – 23	«незадовільно»
24 – 29	«задовільно»
30 – 35	«добре»
36 – 40	«відмінно»

Орієнтовний перелік питань для семестрового контролю

1. Основи моніторингу захищених ІТ систем і мереж.
2. Основні механізми перехоплення трафіка.
3. Принципи моніторингу безпеки ІТ систем.

4. Архітектура DLP-систем.
5. Основні об'єкти та завдання моніторингу ІТ систем.
6. Основні типи DLP систем.
7. Завдання та функції систем моніторингу безпеки.
8. Загальні відомості про DLP системи.
9. Вимоги до систем моніторингу захищених ІТ систем і мереж.
10. Програмні засоби аналізу трафіка.
11. Зміст моніторингу безпеки інформаційних систем.
12. Основи застосування протоколу (SNMP).
13. Завдання, що вирішує моніторинг інформаційної безпеки.
14. Ключові компоненти протоколу SNMP.
15. Основні механізми моніторингу безпеки інформаційної системи.
16. Типовий склад DLP систем.
17. Призначення та склад системи моніторингу подій інформаційної безпеки (SIEM).
18. Функції та джерела інформації системи моніторингу подій інформаційної безпеки (SIEM).
19. Основні методи виявлення мережевих атак шляхом аналізу трафіка.
20. Адміністрування інформаційних систем і політика безпеки ІТС.
21. Заходи щодо адміністрування базових інформаційних служб.
22. Адміністрування за допомогою вбудованих та програмних засобів.
23. Заходи щодо адміністрування базових інформаційних служб.
24. Застосування утиліт NET.EXE та NBTSTAT програми PWLTOOLS.
25. Випадки порушення політики безпеки.
26. Здійснення аналізу причин, що призвели до інциденту, супроводження банку даних таких подій.
27. Розробка та вжиття заходів у разі виявлення спроб НСД до ресурсів АС, порушенні правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів.
28. Забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід із ладу або порушення режимів функціонування.
29. Організація керування доступом до ресурсів АС (розподілення між користувачами необхідних реквізитів захисту інформації – паролів, привілеїв, ключів та ін.).
30. Супроводження й актуалізація бази даних захисту інформації (матриці доступу, класифікаційні мітки об’єктів, ідентифікатори користувачів тощо).
31. Засоби управління доступом.
32. Забезпечення загальної безпеки комп’ютерної системи (мережі).
33. Контроль конфігурації комп’ютерної системи (мережі).
34. Правила, що регламентують сторонні розробки програмного забезпечення.
35. Адресація мережі та архітектура.
36. Керування доступом до мережі.
37. Безпека реєстрації.
38. Телекомунікації та віддалений доступ.
39. Засоби керування доступом.
40. Відповідальність за прикладне програмне забезпечення.
41. Віртуальні приватні мережі, екстра мережі, внутрішні мережі та інші тунелі.
42. Використання електронної пошти для конфіденційного обміну інформацією.
43. Визначення типу захисту від вірусів.
44. Правила експлуатації стороннього програмного забезпечення.
45. Основні підходи до реалізації аудиту безпеки інформації.
46. Заходи щодо аудиту захищених ІТ- систем.
47. Моніторинг стану ІТ систем і мереж з використанням сканерів безпеки.
48. Дослідження засобів перешкоджання аудиту інформації в ІТ системі.
49. Моніторинг поточного функціонування ІТ систем і мереж.
50. Аудит цілісності файлових систем.

51. Проведення аналітичної оцінки поточного стану безпеки інформації в АС.
52. Етапи проведення аудита безпеки захищених комп'ютерних систем та мереж: ініціювання процедури аудита; збирання інформації аудита; аналіз даних аудита; вироблення рекомендацій; підготовка аудиторського звіту.
53. Стандарти, які рекомендується використовувати при проведення аудита безпеки захищених комп'ютерних систем та мереж.
54. Програмні продукти, призначені для аналізу й керування ризиками.
55. Проведення аналітичної оцінки поточного стану безпеки інформації в АС.
56. Інформування власників інформації про технічні можливості захисту інформації в АС і типові правила, встановлені для персоналу й користувачів АС.
57. Негайне втручання в процес роботи АС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт із викриття порушника.
58. Регулярне подання звітів керівництву організації-власника (розпорядника) АС про виконання користувачами АС вимог із захисту інформації.

Шкала відповідності оцінок

Рейтингова оцінка	**Сума балів за всі види навчальної діяльності**	**Значення оцінки**
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов'язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 210 год., лекції – 20 год., практичні заняття – 18 год., лабораторні роботи – 18 год., модульний контроль –12 год., самостійна робота –112 год.

Модулі (назви, бали)	**Змістовий модуль 1. Моніторинг захищених ІТ систем і мереж. (98 балів)**			**Змістовий модуль 2. Адміністрування захищених ІТ систем і мереж (98 балів)**			**Змістовий модуль 3. Аудит захищених ІТ систем і мереж (137 бал)**			
Лекції (теми, бали)	Моніторинг захищених ІТ систем і мереж (1 бал)	Моніторинг безпеки інформаційної системи (1 бал)	Виявлення мережевих атак шляхом аналізу трафіка (1 бал)	Адміністрування інформаційних систем і політика безпеки ІТС (1 бал)	Захист інформації в комп'ютерних мережах, функції адміністратора безпеки (1 бал)	Системи запобігання витоку інформації та виявлення вторгнень (1 бал)	Основні підходи до реалізації аудиту безпеки інформації (1 бал)	Аудит уразливості захищених інформаційно-комунікаційних систем (1 бал)	Аудит інформаційної безпеки із застосуванням методів кластерного аналізу (1 бал)	Заходи щодо аудиту захищених ІТ- систем (1 бал)
Практичні, семінарські заняття (теми, бали)	Моніторинг поточного функціонування ІТ систем і мереж (22 бали)			Принципи використання програмного комплексу SearchInform для контролю просочувань конфіденційної інформації (33 бали)			Аудит ризиків інформаційної безпеки методами найближчого та віддаленого сусіда (22 бали)		Аудит ризиків інформаційної безпеки методом k - середніх (22 бали)	
Лабораторні заняття (теми, бали)	Моніторинг стану ІТ систем і мереж з використанням сканерів безпеки. (33 бали)			Встановлення та налагодження програмного комплексу Searchinform (22 бали)			Аналіз інструментів проведення активного аудиту безпеки (22 бали)		Аудит цілісності файлових систем (22 бали)	
Самостійна робота	Самостійна робота (15 балів)			Самостійна робота (15 балів)			Самостійна робота (20 балів)			
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)			Модульна контрольна робота 2 (25 балів)			Модульна контрольна робота 3 (25 балів)			
Підсумковий контроль (вид, бали)	залік						Екзамен (40 балів)			

8. Рекомендовані джерела

Основна (базова):

1. Богуш В.М., Юдін О.К. Основи інформаційної безпеки держави. – К.: “МК-Прес”, 2005 – 432 с.
2. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
3. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко/ – К. : ДУТ - КНУ, 2016. – 178 с
4. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.
5. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
6. Інформаційна технологія. Методи і засоби забезпечення безпеки. Методологія оцінки безпеки інформаційних технологій - Information technology. Security techniques. Methodology for IT security evaluation : ГОСТ Р ІСО / МЕК 18045-2008. - Х. : ІПК «Видавництво стандартів», 2008. - 234 с.
7. Інформаційна технологія. Методи і засоби забезпечення безпеки. Частина 1. Концепція та моделі менеджменту безпеки інформаційних і телекомунікаційних технологій : ГОСТ Р ІСО / МЕК 13335-1-2006. - Введ. 2007.05.31. - Х.: ІПК «Видавництво стандартів», 2007. - 23 с.
8. Інформаційні технології. Звід правил з управління захистом інформації: ISO/IEC 27002:2005 (E). - Х.: Компанія «Технорматив», 2007. - 117 с.
9. Комп’ютерні мережі: навч. посіб. для технічних спец. вищих навч. закл. Кн. 2. - Львів: Магнолія 2006, 2014. - 327 с.
10. Кононович В.Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж. Загальне користування : Ч. 4. Інформаційна безпека комунікаційних мереж та послуг. Реагування на атаки. Навчальний посібник / В.Г. Кононович, С.В. Гладиш. - Одеса : ОНАЗ ім. О.С. Попова, 2009. - 208 с.
11. Курило А.П. Аудит інформаційної безпеки / Курило А.П. - К. : БДЦ - прес, 2006. - 304 с.
12. Організація щодо реагування на інциденти та обробка інцидентів безпеки : посібник для організації електрозв'язку. Рекомендація МСЕ - Т Е.409 (ITU - T E.409) / Женева. - 22 с. - (Рекомендація Міжнародної організації телекомунікацій).

Додаткова

1. Guidelines for auditing management systems : ISO 9011:2011 // International Organization for Standardization (ISO). - 2011. - 52 p.
2. Herrmann D.S. Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI / D.S. Herrmann. - Auerbach Publications. - 2007. - 824 p. Scott Mueller. Upgrading and Repairing Networks, Third Edition. Que, 2002.
3. International Standard ISO 7498-2: 1989 Information processing systems. - Open Systems Interconnection. - Basic Reference Model. - Part 2: Security Architecture. - First edition. -15.02.1989. - 32 p.ДСТУ 2226--93. Автоматизовані системи. Терміни та визначення.
4. International Standard ISO/IEC 17799. Information technology - Code of practice for information security management. First edition 2000-12-01.
5. Panoc C. Lekkas. Network Processors. The McGraw-Hill Companies, 2003.

9. Додаткові ресурси

1. An improved algorithm for CIOQ switches. Yossi Azar, Ybssi Richter. [електронний ресурс] http://portal.acm.org
2. European Network and Information Security Agency (ENISA) [електронний ресурс] // Режим

доступу: http:// www.enisa.europa.eu.

3. Сайт Інституту інженерів по електротехніці і електроніці (IEEE,Institute of Electrical and Electronics Engineers) [електронний ресурс] http://www.ieee.org

4. Сайт навчальної бази даних «SciVerse ScienceDirect» [електронний ресурс] http://www.sciencedirect.com