МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра кібербезпеки та DATA-технологій, факультет №6

РОБОЧА ПРОГРАМА

навчальної дисципліни «**Моніторинг та аудит кібербезпеки**»
обов'язкових компонент
освітньої програми другого (магістр) рівня вищої освіти

125 «Кібербезпека» (безпека інформаційних та комунікаційних систем)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 22.12.2023 № 11

СХВАЛЕНО
Вченою радою факультету № 6
Протокол від 20.12.2023 № 11

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 21.12.2023 № 11

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій факультету № 6 *(протокол від 15.12.2023 №12)*

Розробник:
Доцент кафедри, к. т. н., доцент Хавіна І.П.

Рецензенти:
1. Професор кафедри комп'ютерних наук та інформаційних технологій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» д. т. н., професор Малєєва О. В.

2. Професор кафедри інформаційних технологій та кібербезпеки ХНУВС, к.т.н., доцент Носов В. В.

1. Опис навчальної дисципліни

Найменування показників	Шифри та назви галузі знань, код та назва спеціальності, ступень вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 3 Загальна кількість годин – 90 Кількість тем – 7	12 Інформаційні технології; (шифр галузі) (назва галузі знань) 125 – Кібербезпека Магістр з кібербезпеки та захисту інформації (назва СВО)	Навчальний курс – 1 Семестр – 2 Види підсумкового контрою: – іспит
Розподіл навчальної дисципліни за видами занять:		
денна форма навчання Лекції – 16 годин; Практичні заняття – 24 годин; Лабораторні заняття – 0 години; Самостійна робота – 50 годин; Індивідуальні завдання: -		заочна форма навчання Лекції – 6 годин; Практичні заняття – 4 годин; Лабораторні заняття – 0 години; Самостійна робота – 80 годин; Індивідуальні завдання: -

2. Мета та завдання навчальної дисципліни

Метою викладання дисципліни «Моніторинг та аудит кібербезпеки» є формування знань, умінь і навичок у здобувачів щодо основних понять, методів, принципів аудиту та моніторингу кібербезпеки в організаціях, установах та підприємствах.

Основними завданнями вивчення дисципліни «Моніторинг та аудит кібербезпеки» є вивчення сучасних методів та технологій забезпечення безпеки інформаційних систем в кібербезпеці. Формування у здобувачів здатності аналізувати та визначати зовнішні та внутрішні загрози в межах інформаційних систем. Формування у здобувачів здатності супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем; Формування у здобувачів здатності розробляти, впроваджувати та аналізувати нормативні документи та положення у галузі моніторингу систем інформаційної безпеки; Формування у здобувачів здатності інтегрувати, аналізувати і використовувати кращі світові практики, стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки; необхідна для курсового та дипломного проектування.

Міждисциплінарні зв’язки: дисципліна «Моніторинг та аудит кібербезпеки» базується на викладання дисциплін «Методика наукових досліджень», «Моделювання складних нелінійних процесів в кібербезпеці», «Розвідувально-аналітична робота у кіберсфері» та освітньої програми першого (бакалаврського) рівня вищої освіти **125 «Кібербезпека».**

Очікувані результати навчання: дисципліна формує компетенції з проблем теорії та практики щодо аналізу, оцінки, методів управління та моніторингу стану захищеності об'єктів інформатизації кібербезпеки на основі сучасних моделей аудиту та моніторингу.У результаті вивчення навчальної дисципліни здобувач вищої освіти повинен:

***знати*:**

- основні поняття і визначення управління інформаційними ризиками;
- основні етапи забезпечення режиму інформаційної безпеки.
- компоненти аналізу ризиків: ідентифікація ризиків (ідентифікація активів, погроз, вразливостей, впливу, засобів контролю) та інше;
- технології аналізу інформаційних ризиків.
- програмні засоби, що використовуються для аналізу і управління ризиками;
- аудит безпеки і аналіз інформаційних ризиків.

вміти:

- знаходити організаційно-управлінські рішення в нестандартних ситуаціях і нести за них відповідальність;
- складати огляд з питань забезпечення інформаційної безпеки за профілем своєї діяльності;
- організовувати і підтримувати виконання комплексу заходів щодо інформаційної безпеки;
- управляти процесом їх реалізації з урахуванням вирішуваних задач і організаційної структури об'єкта захисту, зовнішніх впливів, ймовірних загроз і рівня розвитку технологій захисту інформації;
- здійснювати підбір, вивчення і узагальнення науково-технічної літератури, нормативних та методичних матеріалів з питань забезпечення інформаційної безпеки.

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.	
загальні компетентності (КЗ)	КЗ.1	Здатність застосовувати знання у практичних ситуаціях.
	КЗ.2	Здатність проводити дослідження на відповідному рівні.
	КЗ.3	Здатність до абстрактного мислення, аналізу та синтезу.
	КЗ.4	Здатність оцінювати та забезпечувати якість виконуваних робіт.

	КЗ.5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові Компетентності (КФ)	КФ.1	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
	КФ.2	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 у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
	КФ.3	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури
	КФ.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.
	КФ.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.
	КФ.7	Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
	КФ.8	Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної

		інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
	КФ.9	Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
	КФ.10	Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
Програмні результати навчання (РН)	РН.6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення
	РН.10	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації
	РН.16	Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень
	РН.21	Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки

3. Програма навчальної дисципліни

Тема № 1. Аудит інформаційної безпеки. Термінологія аудиту. Види аудиту. Основні складові системи аудиту інформаційної безпеки. Нормативне забезпечення аудиту інформаційної безпеки.

Тема № 2. Внутрішній аудит СМІБ за вимогами ISO/IEC 27001 та ISO 19011. Загальна характеристика внутрішніх аудитів СМІБ. Принципи проведення внутрішнього аудиту. Управління програмою аудиту. Проведення аудиту. Компетентність аудиторів та її оцінювання.

Тема № 3. Комплексний аудит інформаційної безпеки. Основні етапи аудиту безпеки інформаційних систем. Оцінка діяльності з управління інформаційною безпекою організації.

Тема № 4. Менеджмент інцидентів інформаційної безпеки. Базові принципи, терміни та визначення. Стандарти, рекомендації та найкращі світові практики щодо управління інцидентами інформаційної безпеки. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035. Особливості менеджменту інцидентів відповідно до ITIL. Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки.

Тема № 5. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT в інформаційно-комунікаційних системах. Загальна характеристика діяльності груп CERT/CSIRT. Етапи створення груп CERT/CSIRT. Сервіси, що надаються групами реагування на інциденти інформаційної та кібербезпеки. Обробка інцидентів інформаційної безпеки групами CERT/CSIRT. Документаційне забезпечення процесу управління кіберінцидентам.

4. Структура навчальної дисципліни

4.1.1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 2							
Тема № 1. Аудит інформаційної безпеки	**16**	**2**		**4**		**10**	
Тема № 2. Внутрішній аудит СМІБ за вимогами ISO/IEC 27001 ТА ISO 19011	**18**	**4**		**4**		**10**	
Тема № 3. Комплексний аудит інформаційної безпеки	**20**	**4**		**6**		**10**	
Тема № 4. Менеджмент інцидентів інформаційної безпеки.	**20**	**4**		**6**		**10**	
Тема № 5. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT.	**16**	**2**		**4**		**10**	
Всього по дисципліні	**90**	**16**		**24**		**50**	**Іспит**

4.2. Завдання на самостійну роботу

Завдання що виносяться на самостійну роботу студента			Література:
Семестр № 2			
	Тема 1. Аудит інформаційної безпеки		
		Призначення та склад системи моніторингу подій інформаційної безпеки (SIEM).	Конспект лекцій, література [1-3]
		Архітектура і основні типи DLP-систем Програмні засоби аналізу трафіка	Конспект лекцій, література [1-3]
	Тема 2. Внутрішній аудит СМІБ за вимогами.		
		Життєвий цикл реагування на інциденти NIST	Конспект лекцій, література [1-3]
		Аудит цілісності файлових систем	Конспект лекцій, література [1-3]
	Тема 3. Комплексний аудит інформаційної безпеки.		
		Загальна система оцінки вразливостей (Common Vulnerability	Конспект лекцій, література [1-3]
		Scoring System, CVSS).	Конспект лекцій, література [1-3]
	Тема 4. Менеджмент інцидентів інформаційної безпеки..		
		Особливості менеджменту інцидентів відповідно до ITIL	Конспект лекцій, література [1-3]
		Дослідження засобів перешкоджання аудиту інформації в IT системі	Конспект лекцій, література [1-3]
	Тема 5. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT.		
		Особливості менеджменту інцидентів відповідно до ITIL	Конспект лекцій, література [1-3]
		Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки.	Конспект лекцій, література [1-3]

5. Індивідуальні завдання

6. Методи навчання

Вивчення курсу дозволить здобувачам вищої освіти оволодіти необхідними теоретичними знаннями щодо побудови та принципів функціонування комплексних систем захисту інформації. В навчальному плані для вивчення дисципліни передбачені такі організаційні форми занять як лекції, практичні та лабораторні заняття.

На лекційних заняттях викладаються теоретичні засади тем, що вивчаються, а також приклади їх використання для розв’язання конкретних навчальних задач.

На практичних заняттях під керівництвом викладача слухачі відпрацьовують прийоми виконання типових задач. Практичні заняття проводяться в комп’ютерному класі. Практичні заняття проводяться у здвоєному форматі, що дозволяє більш ефективно використовувати комп’ютерну техніку.

Перед практичним заняттям слухач повинен вивчити певний теоретичний матеріал і (можливо) виконати практичне завдання у відповідності до методичних вказівок до практичних занять з дисципліни. Після закінчення практичного заняття слухач отримує домашнє завдання для закріплення практичних навичок розв’язання задач.

Основним видом інформаційно-методичного забезпечення дисципліни є:

- конспект лекцій;
- методичні вказівки до практичних занять;
- навчальні посібники з дисципліни.

Перелічені складові елементи інформаційно-методичного забезпечення існують як у друкованому вигляді, так і в електронній формі у вигляді роздаткових матеріалів, відповідного розділу сайту кафедри кібербезпеки та інформаційних систем, а також у вигляді електронного навчального комплексу з дисципліни у системі ДО ХНУВС.

7. Перелік питань та завдань, що виносяться на підсумковий контроль

1. Що таке аудит?
2. Що означає аудит першої сторони, аудит другої сторони, аудит третьої сторони?
3. Що таке система менеджменту інформаційної безпеки?
4. Розтлумачте різницю між поняттями «критерії аудиту», «дані аудиту», «спостереження аудиту».
5. За якими показниками визначається обсяг аудиту?
6. У чому різниця між поняттями подія в системі захисту інформації та інцидент в системі захисту інформації?
7. Які види аудиту Ви знаєте?
8. Для чого проводиться діагностичний аналіз?
9. Що таке експертний аудит, в яких випадках він проводиться?
10. Що таке аудит ІБ на відповідність міжнародним стандартам, у яких випадках він проводиться?
11. Розтлумачте сутність активного аудиту. З якою метою він проводиться?
12. Що таке опитувальник Bridge Point? Для чого він призначений?
13. Якою є основна мета аудиту?
14. Розкрийте завдання та цілі аудиту.
15. Назвіть основні принципи аудиту.
16. Порівняйте стандарти CobiT, ITIL, ISO/IEC 15408, ISO/IEC 270XX. Для яких цілей вони призначені, у чому особливості їх застосування в галузі ІБ?

17. Якими стандартами слід керуватись при організації та проведенні аудиту СМІБ?
18. Назвіть основні етапи проведення внутрішніх аудитів СМІБ.
19. Назвіть критерії, що впливають на тривалість внутрішнього аудиту.
20. Які особливості укладання опитувальників для проведення внутрішнього аудиту Ви знаєте?
21. Перелічіть основні складові стандартного пакету аудитора.
22. Що таке відхилення (невідповідності)? Дайте визначення критичним та некритичним невідповідностям.
23. Вкажіть основні причини відхилень, які виявляються під час внутрішнього аудиту.
24. Назвіть основні етапи усунення невідповідностей.
25. Які принципи проведення внутрішнього аудиту Ви знаєте?
26. Які основні відомості повинна містити програма аудиту?
27. Чим відрізняється програма аудиту від плану аудиту?
28. Назвіть основні етапи управління програмою аудиту відповідно до стандарту ISO 19011.
29. Залежно від чого формуються цілі програми аудиту?
30. Від чого залежить обсяг програми аудиту?
31. Якими можуть бути ризики для програми аудиту?
32. Які процедури слід врахувати особі, що здійснює управління програмою аудиту, при її складанні?
33. Які ресурси слід передбачити у програмі аудиту?
34. Що таке цілі, сфера та критерії конкретного аудиту? Якими показниками характеризується сфера аудиту?
35. Назвіть основні типи аудиторів та інших суб'єктів, які можуть залучатися до проведення аудиту. Які обов'язки покладаються на кожного з них?
36. Вкажіть основні форми записів, які визначаються програмою аудиту.
37. З якою метою проводять моніторинг виконання програми аудиту?
38. Назвіть типові дії при проведенні аудиту. Чи може змінюватись їх порядок? Чим він визначається?
39. Яка інформація повідомляється під час вступної наради? Кого на неї запрошують?
40. Назвіть види робочих документів, призначених для реєстрації зібраної під час проведення аудиту інформації.
41. З якою метою проводиться аналіз документів під час проведення аудиту?
42. Назвіть основні етапи процесу збирання та перевірки інформації.
43. Чим відрізняються результати аудиту від висновків аудиту?
44. Яка інформація повідомляється під час підсумкової наради?
45. Які відомості відображається у звіті про проведення аудиту?
46. Для чого оцінювати компетентність аудиторів?
47. Якими є кількісні та якісні критерії оцінювання компетентності аудиторів?
48. Назвіть методи оцінювання компетентності аудиторів.
49. Як аудитори можуть підвищувати власну компетентність?
50. Назвіть ключові елементи комплексного аудиту інформаційної безпеки.

51. Які основні етапи аудиту безпеки інформаційних систем Ви знаєте?
52. Які характеристики побудови і функціонування ІС аналізуються на етапі збору та аналізу даних?
53. Які джерела інформації та способи збору даних використовуються під час аудиту безпеки інформаційних систем?
54. Що є результатом етапу аналізу ризиків ІС під час аудиту?
55. Які відомості містить звіт за результатами аудиту безпеки інформаційних систем?
56. Розтлумачте поняття «вимірювання», «показники» і «метрика безпеки».
57. Для чого призначений стандарт ISO/IEC 27004:2009? Який його недолік?
58. Назвіть основні етапи та складові програми оцінювання ефективності СМІБ.
59. Надайте коротку характеристику моделі оцінювання ефективності СМІБ.
60. Що означають поняття «базовий показник», «похідний показник», «метод вимірювання», «формула обчислень», «критерії прийняття рішень», «результат вимірювання» у процесі оцінювання ефективності СМІБ?
61. Назвіть основних суб'єктів оцінювання ефективності СМІБ та їх обов'язки.
62. Визначте роль СМІІБ у системі забезпечення інформаційної безпеки організації. Які завдання повинна вирішувати СМІІБ організації?
63. Якими є цілі управління інцидентами інформаційної безпеки?
64. Назвіть основні заходи щодо створення СМІІБ.
65. Розтлумачте різницю між поняттями подія ІБ та інцидент ІБ.
66. Визначте загальні вимоги до побудови процесів управління інформаційною безпекою.
67. Що таке управління інцидентами інформаційної безпеки? Назвіть основні його складові.
68. Від чого залежить ефективність процесу УІІБ?
69. Які ознаки інциденту інформаційної безпеки Ви знаєте?
70. Які заходи проводяться в процесі УІІБ?
71. Назвіть основні міжнародні та національні нормативні документи, якими визначаються процедури УІІБ.
72. Сформулюйте основний принцип застосування міжнародні та національні стандартів, що описують УІІБ.
73. Для чого організації необхідні нормативні документи з УІІБ?
74. Наведіть приклади ІІБ організації.
75. Назвіть етапи розробки СМІІБ відповідно до моделі PDCA.
76. Визначте основні етапи управління інцидентами ІБ та охарактеризуйте їх.
77. У чому полягає особливість підходу управління інцидентами ІБ відповідно до ITIL?
78. Назвіть основні складові моделі інцидентів відповідно до ITIL.
79. Що означає поняття «вирішити інцидент»? Назвіть основні складові процесу вирішення інциденту.
80. Охарактеризуйте основні етапи управління інцидентами відповідно до ITIL.
81. Які відомості повинен містити запис про інцидент відповідно до ITIL?
82. У чому полягає сутність категорування інцидентів? Для чого необхідна ця процедура?

83. Розтлумачте поняття «вплив», «терміновість», «пріоритет». Чому ці поняття важливі і для чого використовуються ці характеристики?
84. Як визначити норми часу для обробки інциденту?
85. Розтлумачте поняття «ескалація». У чому полягає процес ескалації і якою є мета застосування цієї процедури?
86. Які характеристики можуть бути використані як метрики ефективності процесу управління інцидентами?
87. У чому полягає процедура закриття інциденту?
88. Що є ризиками для процесу управління інцидентами?
89. Назвіть етапи впровадження СМІБ.
90. Вкажіть основні складові автоматизованої системи моніторингу й управління інцидентами інформаційної безпеки.
91. Що таке команда CERT/CC? Які її основні завдання?
92. Що таке CERT/CSIRT, FIRST і для чого вони призначені?
93. Охарактеризуйте діяльність CERT-UA та особливості її функціонування.
94. Які види CERT/CSIRT відповідно до галузевих ознак Ви знаєте?
95. Назвіть основні етапи створення CERT/CSIRT.
96. Які типи організаційної структури CERT/CSIRT Ви знаєте?
97. Охарактеризуйте розподіл ролей і функцій членів команд CERT/CSIRT.
98. Розкрийте сутність базових сервісів, які надаються командами CERT/CSIRT.
99. У чому полягають додаткові сервіси CERT/CSIRT?
100. У чому полягає порядок обробки інцидентів групою CERT/CSIRT?
101. Яким чином і з якою метою здійснюється оцінка збитків, завданих інцидентами ІБ?
102. Як організувати зберігання матеріалів розслідування інцидентів інформаційної безпеки?
103. Які ресурси та засоби необхідні для розслідування ІІБ?
104. Охарактеризуйте основні типи документів, необхідні для організації роботи групи CERT/CSIRT.

8. Розподіл балів, які отримують здобувачі вищої освіти з навчальної дисципліни

Контрольні заходи включають у себе поточний та підсумковий контроль.

Поточний контроль.

До форм поточного контролю належить оцінювання:

- рівня знань під час практичних, лабораторних занять;
- якості виконання індивідуальної та самостійної роботи.

Поточний контроль здійснюється під час проведення практичних та лабораторних занять і має за мету перевірку засвоєння знань, умінь і навичок здобувачем вищої освіти з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до

журналів обліку роботи академічної групи за національної системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну та індивідуальну роботи виставляються в журнали обліку роботи академічної групи в окрему графу за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів вищої освіти в Університеті враховуються такі види робіт: навчальні заняття (практичні, лабораторні тощо); самостійна та індивідуальна роботи (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп'ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у вигляді, передбаченому в робочій програмі навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Результат навчальних занять за семестр розраховується як середньоарифметичне значення з усіх виставлених оцінок під час навчальних занять протягом семестру та виставляється викладачем в журналі обліку роботи академічної групи в окрему графу.

Результат самостійної роботи за семестр розраховується як середньоарифметичне значення з усіх виставлених оцінок з самостійної роботи, отриманих протягом семестру та виставляється викладачем в журналі обліку роботи академічної групи в окрему графу.

Здобувач вищої освіти***, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов'язаний його відпрацювати.***

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середньоарифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переводу до 100-бальної системи помножується на коефіцієнт **10**.

Загальна кількість балів (перед підсумковим контролем)	**=((**	***Результат навчальних занять за семестр***	**+**	***Результат самостійної роботи за семестр***	**) /**	***2)***	****10***

Підсумковий контроль.

Підсумковий контроль проводиться з метою оцінки результатів навчання на певному ступені вищої освіти або на окремих його завершених етапах.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструються в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображуються у відомостях обліку успішності, навчальних картках курсантів (студентів, слухачів), залікових книжках. ***Присутність курсантів (студентів, слухачів) на проведенні підсумкового контролю (заліку, екзамену) обов'язкова.*** Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік, екзамен), то науково-педагогічний працівник ставить у відомість обліку

успішності відмітку «не з’явився».

Підсумковий контроль (екзамен, залік) оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі (екзамені, заліку), з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (екзамені, заліку), які використовуються при розрахунку успішності курсантів (студентів, слухачів), становить – **50.**

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру та балів, набраних на підсумковому контролі (екзамені, заліку).

$$\textit{Підсумкові бали навчальної дисципліни} = \textit{Загальна кількість балів (перед підсумковим контролем)} + \textit{Кількість балів за підсумковим контролем}$$

Здобувач вищої освіти, який під час складання підсумкового контролю отримав оцінку «незадовільно», складає підсумковий контроль (екзамен, залік) повторно. Повторне складання підсумкового контролю (екзамену, заліку) допускається не більше двох разів з кожної навчальної дисципліни, у тому числі один раз – викладачеві, а другий – комісії, що створюється навчально-науковими інститутами (факультетами). Незадовільні оцінки виставляються тільки в відомостях обліку успішності. Студентам, які отримали не більше як дві незадовільні оцінки (нижче ніж 60 балів) з навчальної дисципліни, можуть бути встановлені різні строки ліквідації академічної заборгованості, але не пізніше як за день до фактичного початку навчальних занять у наступному семестрі. Студенти, які не ліквідували академічну заборгованість у встановлений термін, відраховуються з Університету. Особи, які одержали більше двох незадовільних оцінок (нижче ніж 60 балів) за підсумковими результатами вивчення навчальних дисциплін з урахуванням підсумкового контролю, відраховуються з Університету.

Результат вивчення дисципліни визначається як середньоарифметичне значення балів, набраних у поточному та попередньому семестрах.

$$\textit{Підсумкові бали навчальної дисципліни} = \frac{\textit{Підсумкові бали за поточний семестр} + \textit{Підсумкові бали за попередній семестр}}{2}$$

Кафедрою визначено наступні критерії оцінювання результатів роботи здобувачів вищої освіти під час поточного контролю (роботу на семінарських, практичних, лабораторних й інших аудиторних заняттях, виконання самостійних навчальних та індивідуальних творчих завдань) та підсумкового контролю.

Робота під час навчальних занять	Самостійна та індивідуальна робота	Підсумковий контроль
Отримати не менше 4 позитивних оцінок (денна форма навчання)	Підготувати реферат, підготувати конспект за темами самостійної роботи.	Отримати за підсумковий контроль не менше 30 балів

9. Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка	
		Оцінка	Пояснення
97-100 94-96 90-93	Відмінно («зараховано»)	A	«**Відмінно"** – теоретичний зміст курсу засвоєний **цілком,** необхідні практичні навички роботи з освоєним матеріалом сформовані, **усі** навчальні завдання, які передбачені програмою навчання **виконані** в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
85- 89 80-84	Добре («зараховано»)	B	«**Дуже добре"** – теоретичний зміст курсу засвоєний **цілком**, потрібні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **усі** навчальні завдання, які передбачені програмою навчання, **виконані**, якість виконання **більшості** з них оцінена числом балів, близьким до **максимального,** робота з двома-трьома незначними помилками.
75-79		C	«**Добре"** – теоретичний зміст курсу засвоєний **цілком**, практичні навички роботи з освоєним матеріалом **в основному** сформовані, **усі** навчальні завдання, які передбачені програмою навчання, **виконані**, якість виконання **жодного** з них **не оцінена мінімальним** числом балів, деякі види завдань виконані **з помилками,** робота з декількома незначними помилками, або з однією-двома значними помилками.
70 -74 65-69	Задовільно («зараховано»)	D	«**Задовільно"** – теоретичний зміст курсу засвоєний **частково**, але **прогалини не носять істотний** характер, потрібні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **більшість** передбачених програмою навчання навчальних завдань **виконана, деякі** з виконаних завдань містять **помилки,** робота з трьома значними помилками.
60-64		E	«**Достатньо"** – теоретичний зміст курсу освоєний **частково, деякі** практичні навички роботи **не сформовані, частина** передбачених програмою навчання навчальних завдань **не виконана,** або якість виконання деяких з них оцінена числом балів, близьким до **мінімального**, робота, що задовольняє мінімуму критеріїв оцінки.
41-59 21-40	Незадовільно («не зараховано»)	FX	«**Умовно незадовільно"** – теоретичний зміст курсу засвоєний **частково**, потрібні практичні навички роботи **несформовані, більшість** передбачених програмою навчання, навчальних завдань **не виконано**, або якість їхнього виконання оцінено числом балів, близьким до **мінімального**; при **додатковій самостійній** роботі над матеріалом курсу **можливе підвищення якості** виконання навчальних завдань (**з можливістю повторного складання**), робота, що потребує доробки.
1-20		F	«**Безумовно незадовільно"** – теоретичний зміст курсу **неосвоєний**, потрібні практичні навички роботи **несформовані, всі виконані** навчальні завдання містять грубі **помилки, додаткова самостійна** робота над матеріалом курсу **не приведе** до значного **підвищення якості** виконання навчальних завдань, робота, що потребує повної переробки.

10. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна література

1. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 193 с.
2. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с.
3. 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.

Допоміжна література

1. Метод формування параметрів функціональних обов'язків для оцінки загроз в соціотехнічних системах/ А. Корченко, С. Мацюк, О. Чобаль, О. Кручінін, Т. Паращук// Information Technology: Computer Science, Software Engineering and Cyber Security. – 2022. – №3. – С. 19-26.
2. Кількісна оцінка кіберзахищеності інформації/ В. Хорошко Ю. Хохлачова, Н. Вишневська, О. Чобаль// Захист інформації. – 2023. – Т.25 (№2). – С. 70-76.
3. Стандарти систем управління ІБ серії ISO/IEC 27000. [Електронний ресурс]. Режим доступу: https://www.iso27001security.com/

Інформаційні ресурси в мережі Інтернет

1. https://www.netacad.com/
2. https://www.splunk.com/
3. https://portal.rangeforce.com/