МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра інформаційних технологій та кібербезпеки факультету № 4

РОБОЧА ПРОГРАМА

навчальної дисципліни " Вступ у спеціальність "
вибіркових компонент
освітньої програми першого (бакалаврського) рівня вищої освіти

125 "Кібербезпека" (Безпека інформаційних та комунікаційних систем)

Харків 2020

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 23.09.2020 № 9

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 16.09.2020 № 5

ПОГОДЖЕНО
Секцією науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 18.09.2020 № 5

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки (протокол від 15.09.2020 № 16)

Розробник: доцент кафедри інформаційних технологій та кібербезпеки факультету №4 Харківського національного університету внутрішніх справ, к.т.н. доцент Тулупов В.В.

Рецензенти:
професор кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ, к.т.н. доцент Носов В.В.

професор кафедри проектування та експлуатації електронних апаратів Харківського національного університету радіоелектроніки, к.т.н. доцент Хорошайло Ю.Є.

1. Опис навчальної дисципліни

Найменування показників	Шифри та назви галузі знань, код та назва спеціальності, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 3 Загальна кількість годин – 90 Кількість тем – 11	12 - Інформаційні технології 125 - Кібербезпека (Безпека інформаційних та комунікаційних систем) бакалавр	Навчальний курс-1 Семестр -1 Види контрою - залік
Розподіл навчальної дисципліни за видами занять:		
денна форма навчання Лекції – 24; (години) Практичні заняття – 22 ; (години) Самостійна робота – 44; (години) Індивідуальні завдання: Реферати (тощо) – 1	заочна форма навчання	

2. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни «Вступ у спеціальність» є вивчення сучасних вимог до інформаційної безпеки, її зв'язку з юридичними, суспільними та природничими науками; концептуальний підхід до питань функціонування і структурної побудови системи інформаційного забезпечення та захисту, засвоєння курсантами теоретичних основ протидії кіберзлочинності, що дозволить фахівцям розуміти принципи та методи боротьби з цим явищем.

Основними завданнями вивчення дисципліни «Вступ у спеціальність» є: узагальнення передового досвіду роботи фахівців в сфері інформаційної безпеки щодо стандартизації, уніфікації методів, способів, засобів і заходів забезпечення кібербезпеки.

Міждисциплінарні зв'язки: «Правознавство», «Інформаційні технології», «Комп'ютерні основи систем кібербезпеки», «Кібербезпека», «Управління та організація в сфері інформаційної безпеки», «Правові засади кібербезпеки», «Комплексні системи захисту інформації: проектування, впровадження, супровід», «Методи та засоби захисту інформації».

Очікуванні результати навчання: у результаті вивчення навчальної дисципліни здобувач вищої освіти повинен:

знати:

особливості поширення інформації; можливості сучасних інформаційних технологій; теоретичні основи інформаційної безпеки; правове регулювання забезпечення інформаційних відносин, а також інформаційної безпеки особистості, суспільства, держави; стандартизацію, уніфікацію методів, способів, засобів і заходів забезпечення кібербезпеки;

вміти:

орієнтуватися в сучасних автоматизованих засобах інформаційного і довідкового забезпечення завдань юридичної практики, їхнього призначення і методів використання; самостійно вирішувати практичні задачі щодо забезпечення безпеки інформаційних ресурсів і засобів їхньої обробки в єдиному інформаційному просторі (кіберпросторі); формулювати рекомендації щодо розробки механізму реалізації, науково-практичних пропозицій і рекомендацій з підвищення ефективності правового та організаційного управління забезпеченням інформаційної безпеки.

Програмні компетентності, які формуються при вивченні навчальної дисципліни:	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційних технологій (кібербезпека), що передбачає ідентифікацію та використання інформації для прийняття рішень
Загальні компетентності (ЗК)	ЗК 2. Здатність застосовувати знання на практиці. ЗК 3. Знання та розуміння предметної області та розуміння професії. ЗК 6. Здатність до пошуку, обробки та аналізу інформації з різних джерел.
Фахові компетентності (ФК)	ФК1. Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності.

3.Програма навчальної дисципліни

Тема № 1. Законодавство в сфері забезпечення інформаційної безпеки

Інформаційна безпека: поняття, структура, зміст. Державна політика України в сфері інформатизації та інформаційної безпеки особистості, суспільства, держави, сучасних автоматизованих і телекомунікаційних систем. Класифікація та структура нормативних правових актів в сфері інформаційної безпеки України. Міжнародне законодавство в сфері захисту інформації.

Тема № 2. Основні положення інформаційної безпеки

Визначення інформаційної безпеки. Предмет, об'єкт і суб'єкти інформаційної безпеки. Види інформаційної безпеки. Концепція інформаційної безпеки держави. Поняття і види інформації, що захищається по законодавству України. Державна таємниця як особливий вид інформації, що захищається.

Тема № 3. Правові питання захисту інформації з використанням технічних засобів

Особливості правового регулювання суспільних відносин при використанні технічних засобів обробки інформації та при розробці шифрувальних засобів. Правове регулювання

захисту інформації в засобах зв'язку. Правове регулювання використання цифрового підпису і захисту інформації в системах і засобах електронного документообігу.

Тема № 4. Загрози інформаційній безпеці

Класифікація загроз інформаційній безпеці. Джерела загроз інформаційній безпеці. Методи і засоби забезпечення інформаційної безпеки: основні принципи, система забезпечення, основні фактори і способи. Класифікація загроз безпеці інформації. Класифікація уразливостей безпеці інформації. Вибір стратегії зменшення загроз безпеці інформації.

Тема № 5. Юридична відповідальність за порушення правових норм в галузі інформаційної безпеки

Поняття і види юридичної відповідальності за порушення правових норм в сфері інформаційної безпеки. Кримінальна відповідальність за порушення правових норм в сфері інформаційної безпеки. Адміністративна відповідальність за порушення правових норм в сфері інформаційної безпеки. Особливості юридичної відповідальності за порушення правових норм інформаційної безпеки в галузі трудових норм і цивільно-правових відносин.

Тема № 6. Загальна характеристика каналів витоку інформації

Відкриті джерела інформації. Напрями одержання відкритого доступу до конфіденційної інформації. Етапи аналітичної роботи з інформацією: інтерпретація інформації, виділення сторонньої інформації, оцінка інформації, побудова попередніх версій, вивчення потреби в додатковій уточнюючій інформації, підготовка аналітичних звітів. Технічні канали витоку інформації. Поняття та класифікація технічних каналів витоку інформації (ТКВІ). Акустичні канали витоку інформації. Канали витоку інформації за рахунок побічних електромагнітних випромінювань і наведень ((ПЕМВН) засобів електронно-обчислювальної техніки.

Тема № 7. Методи та засоби захисту інформації в комп'ютерних системах

Загальна характеристика загальних вимог безпеки. Класи функціональних вимог безпеки: аудит, захист інформації, ідентифікація та автентифікація, керування безпекою, контроль доступу до системи, контроль за використанням ресурсів, конфіденційність роботи в системі, криптографія, надійність засобів захисту. Загальна характеристика вимог гарантій безпеки.

Тема № 8. Основи управління інформаційною безпекою

Стандарти менеджменту інформаційної безпеки ти їх основні положення. Політика інформаційної безпеки організації. Концепція інформаційної безпеки організації. Основні правила інформаційної безпеки організації. Правила розмежування доступу користувачів та процесів до ресурсів інформаційної сфери організації.

Тема № 9. Загальні методи забезпечення інформаційної безпеки

Правові методи забезпечення інформаційної безпеки. Організаційно-технічні методи забезпечення інформаційної безпеки. Економічні методи забезпечення інформаційної безпеки. Забезпечення інформаційної безпеки у загальнодержавних і телекомунікаційних системах. Забезпечення інформаційної безпеки у правоохоронній та судових сферах.

Тема № 10. Засадничі принципи боротьби з кіберзлочинністю
Основні відомості про кібербезпеку. Терміни та визначення. Принципи безпеки. Об'єкти та суб'єкти боротьби з кіберзлочинністю. Організаційно-правові засади боротьби з кіберзлочинністю.

Тема № 11. Методи боротьби з кіберзлочинністю в Україні
Міжнародний досвід боротьби з кіберзлочинністю. Розслідування інцидентів порушення комп'ютерної безпеки у приватних компаніях

4. Структура навчальної дисципліни

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

Номер та найменування тем	Кількість годин відведених на вивчення навчальної дисципліни						Література, сторінки	Вид контролю
	Всього	з них:						
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота		
Тема № 1. Законодавство в сфері забезпечення інформаційної безпеки	8	2	–	2	–	4	1,4,5-7,10,11,15,16,17,18,2021,22,26	
Тема№2. Основні положення інформаційної безпеки	6	2	–	2	–	4	11,15,18, 22,23,28,31-34	
Тема № 3. Правові питання захисту інформації з використанням технічних засобів	6	2	–	2	–	4	10,12,14,19, 7	
Тема № 4. Загрози інформаційній безпеці, безпеці інформації та інформаційних ресурсів	6	2	–	2	–	4	14	
Тема № 5. Юридична відповідальність за порушення правових норм в сфері інформаційної безпеки	8	2	–	2	–	4	1,3-5,6,9,11,32	
Тема № 6. Загальна характеристика каналів витоку інформації	8	2	–	2	–	4	29,31	
Тема № 7. Методи та засоби захисту інформації в комп'ютерних системах	6	2	–	2	–	4	29,31,	
Тема № 8. Основи управління інформаційною безпекою	6	2	–	2	–	4	29,31,	

Тема № 9. Загальні методи забезпечення інформаційної безпеки	8	2	–	2	–	4	29,31	
Тема № .10 Засадничі принципи боротьби з кіберзлочинністю	8	2	-	2		4	1,4-21	
Тема № 11. Методи боротьби з кіберзлочинністю в Україні	10	4	-	2		4	1, 22-29	
Всього	**90**	**24**		**22**		**44**		**залік**

4.1.2. Питання, що виносяться на самостійне опрацювання

Перелік питань до тем навчальної дисципліни	**Література:**
Тема № 1: Законодавство в сфері забезпечення інформаційних відносин	
Захист персональних даних і відомостей про приватне життя громадян	1,4,5-7,10,11,15,16,17,18,2021,22,26,39,40
Тема № 2: Основні положенні інформаційної безпеки	
Життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері	11,15,18, 22,23,28,31-34,37,39,40
Тема № 3: Правові питання захисту інформації з використанням технічних засобів	
Засоби боротьби із закладними пристроями прослуховування	10,12,14,19,35,3638,39,46,47
Тема № 4: Загрози інформаційній безпеці, безпеці інформації та інформаційних ресурсів	
Дестабілізуючі фактори інформаційної безпеки	14,35,36,38,41,49-51
Тема № 5: Юридична відповідальність за порушення правових норм в сфері інформаційної безпеки	
Службова та професійна таємниця в системі забезпечення інформаційної безпеки	1,3-5,6,9,11,32,37,39,48
Тема № 6: Загальна характеристика каналів витоку інформації	
Суб'єкти – носії інформації (персонал)	29,31,35,36,41,49,50
Тема № 7: Методи та засоби захисту інформації в комп'ютерних системах	
Етапи аналітичної роботи з інформацією	29,31,35,36,41,49,50
Тема № 8: Основи управління інформаційною безпекою	
Загальні вимоги до захищеності комп'ютерних систем від несанкціонованої зміни структур	29,31,35,36,41,49,50
Тема № 9: Загальні методи забезпечення інформаційної безпеки	
Підходи до оцінки ефективності комплексних систем захисту інформації	29,31,35,36,41,49,50
Тема №10. Засадничі принципи боротьби з кіберзлочинністю	
Об'єкти та суб'єкти боротьби з кіберзлочинністю. Самостійно дослідити нормативно-правові акти, як	1,4-21

регламентують боротьбу з кіберзлочинністю	
Організаційно-правові засади боротьби з кіберзлочинністю. Дослідити схеми вчинення кіберзлочинів та запропонувати власні методи боротьби з ними	1,22-26
Тема № 11. Методи боротьби з кіберзлочинністю в Україні	
Методи боротьби з кіберзлочинністю в Україні Підготувати реферат про досвід боротьби з кіберзлочинністю у одній з країн, не відзначеній у лекційному курсі	1, 22-27
Розслідування інцидентів порушення комп'ютерної безпеки у приватних компаніях. Дослідити методику розслідування інцидентів порушення комп'ютерної безпеки від компанії Microsoft	1, 22-27

5. Індивідуальні завдання

5.1.1.Теми рефератів

1. Правове регулювання в сфері безпеки інформації.
2. Конституційні гарантії прав громадян на інформацію, механізм її реалізації.
3. Основні положення державної інформаційної політики.
4. Національні інтереси України в сфері інформаційної безпеки.
5. Стан інформаційної безпеки України
6. Напрями державної політики України в сфері інформатизації та інформаційної безпеки особистості, суспільства, держави.
7. Боротьба з кіберзлочинністю у Франції.
8. Система боротьби з кіберзлочинністю у арабських країнах.
9. Африканський досвід протидії кіберзлочинам.
10. Протидія кіберзлочинам у країнах Латинської Америки.
11. Австралійський досвід боротьби з кіберзлочинністю.
12. Основні поняття та стандарти інформаційної безпеки.
13. Основні тенденції розвитку інформаційних технологій
14. Юрисдикція у кіберпросторі.
15. Міжнародна взаємодія у боротьбі з кіберзлочинністю.
16. Типові помилки і порушення законодавства, що допускаються при виявленні та документуванні кіберзлочинів.
17. Потенційні загрози безпеці та типові завдання захисту.
18. Основні напрями забезпечення безпеки інформації та інформаційних ресурсів.
19. Міжнародне співробітництво України в сфері забезпечення інформаційної безпеки.
20. Конвенція про кіберзлочинність як базовий документ для міжнародного співробітицтва.
21. Особливості придбання спеціальних технічних засобів для боротьби з кіберзлочинністю за кордоном.
22. Нетрадиційні методи розкриття кіберзлочинів.

6. Методи навчання

Аудиторні заняття проводяться у формі візуального представлення аналітично-графічного матеріалу дисципліни, на яких студенти повинні виконувати відповідні розумові, обчислювальні та практичні дії.

Самостійна робота за кожною темою передбачає вивчення теоретичних питань лекційних занять, опрацювання завдань практичних занять. Індивідуальна робота передбачає написання рефератів.

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

Контроль проводиться по тестових завданнях на підсумковому контролі – заліку.

1. Інформаційна безпека: поняття, структура, зміст.
2. Державна політика України в сфері інформатизації та інформаційної безпеки особистості, суспільства, держави, сучасних автоматизованих і телекомунікаційних систем.
3. Класифікація та структура нормативних правових актів в сфері інформаційної безпеки України.
4. Міжнародне законодавство в сфері захисту інформації.
5. Визначення інформаційної безпеки.
6. Предмет, об’єкт і суб’єкти інформаційної безпеки. Види інформаційної безпеки.
7. Концепція інформаційної безпеки держави.
8. Поняття і види інформації, що захищається по законодавству України.
9. Державна таємниця як особливий інформації, що захищається.
10. Особливості правового регулювання суспільних відносин при використанні технічних засобів обробки інформації та при розробці шифрувальних засобів.
11. Правове регулювання захисту інформації в засобах зв’язку.
12. Правове регулювання використання цифрового підпису і захисту інформації в системах і засобах електронного документообігу.
13. Класифікація загроз інформаційній безпеці.
14. Ієрархічна класифікація загроз інформаційній безпеці.
15. Джерела загроз інформаційній безпеці особистості.
16. Джерела загроз інформаційній безпеці суспільства.
17. Джерела загроз інформаційній безпеці держави.
18. Основні принципи забезпечення інформаційної безпеки.
19. Система забезпечення інформаційної безпеки. Держави.
20. Основні форми і способи забезпечення інформаційної безпеки держави.
21. Методи і засоби забезпечення інформаційної безпеки: основні принципи, система забезпечення, основні фактори і способи.
22. Класифікація загроз безпеці інформації.
23. Ранжування джерел загроз безпеці інформації.
24. Методи ранжування загроз безпеці інформації.
25. Класифікація уразливостей безпеці інформації.
26. Ранжування уразливостей.
27. Класифікація актуальних загроз безпеці інформації.
28. Вибір стратегії зменшення загроз безпеці інформації.
29. Поняття і види юридичної відповідальності за порушення правових норм в сфері інформаційної безпеки.

30. Кримінальна відповідальність за порушення правових норм в сфері інформаційної безпеки.
31. Адміністративна відповідальність за порушення правових норм в сфері інформаційної безпеки.
32. Особливості юридичної відповідальності за порушення правових норм інформаційної безпеки в сфері трудових норм і цивільно-правових відносин.
33. Технічні канали витоку інформації.
34. Поняття та класифікація технічних каналів витоку інформації (ТКВІ).
35. Акустичні канали витоку інформації.
36. Канали витоку інформації за рахунок побічних електромагнітних випромінювань і наведень (ПЕМВН) засобів електронно-обчислювальної техніки.
37. Основні поняття про стандарти інформаційної безпеки.
38. Основні положення загальних критеріїв безпеки інформаційних технологій.
39. Критерії безпеки комп'ютерних систем.
40. Європейські критерії безпеки інформаційних технологій.
41. Федеральні критерії інформаційних технологій.
42. Канадські критерії інформаційних технологій.
43. Загальна характеристика організаційних методів захисту інформації в комп'ютерних системах.
44. Захист інформації в комп'ютерних системах від випадкових загроз.
45. Методи і засоби захисту від електромагнітних випромінювань і наводок.
46. Захист інформації в комп'ютерних системах від несанкціонованого доступу.
47. Комп'ютерні віруси і методи боротьби з ними.
48. Захист інформації в розподілених системах.
49. Концепція організації захищених комп'ютерних систем.
50. Етапи створення комплексної системи захисту комп'ютерних систем.
51. Науково-дослідницька розробка комплексної системи захисту інформації.
52. Вибір показників ефективності та критеріїв оптимальності комплексної системи захисту інформації.
53. Створення організаційної структури комплексної системи захисту інформації.
54. Організація функціонування комплексних систем захисту інформації.
55. Правові методи забезпечення інформаційної безпеки.
56. Організаційно-технічні методи забезпечення інформаційної безпеки.
57. Економічні методи забезпечення інформаційної безпеки.
58. Забезпечення інформаційної безпеки у загальнодержавних і телекомунікаційних системах.
59. Забезпечення інформаційної безпеки у правоохоронній та судових сферах.
60. Технічна експлуатація комплексних систем захисту інформації.
61. Поняття та способи вчинення кіберзлочинів.
62. Нормативно-правова база боротьби з кіберзлочинністю.
63. Суб'єкти боротьби з кіберзлочинністю.
64. Завдання підрозділів боротьби з кіберзлочинністю.
65. Функції підрозділів боротьби з кіберзлочинністю.
66. Типові схеми здійснення кіберзлочинів.
67. Визначення поняття «кіберпростір», його ознаки.
68. Вчинення злочинів через кіберпростір.
69. Питання визначення компетенції правоохоронних органів у кіберпросторі.
70. Шляхи конвергенції організованої злочинності та кіберпростору.

71. Цілодобова мережа для здійснення контактів з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення.
72. Український досвід регулювання питання здійснення оперативно-розшукових заходів шляхом використання кіберпростору.
73. Органи боротьби з кіберзлочинністю в різних країнах.
74. Боротьба зі злочинністю з використанням комп’ютерних технологій у російському законодавстві та в теорії оперативно-розшукової діяльності.
75. Інструменти здійснення оперативно-розшукових заходів через кіберпростір у США.
76. Зміст онлайнової секретної операції в США.
77. Правила онлайнових розслідувань США.
78. Боротьба з кіберзлочинністю у ФРН та загальний порядок здійснення проникнення за допомогою технічних засобів у інформаційно-технічні системи, що використовуються підозрюваним.
79. Використання комп’ютерних технологій в оперативно-розшуковій діяльності Великої Британії та КНР.
80. Службові розслідування інцидентів порушення комп’ютерної безпеки у приватних компаніях.

8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи включають у себе поточний та підсумковий контроль.

Поточний контроль.

До форм поточного контролю належить оцінювання:

- рівня знань під час практичних і 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 (далі – здобувач) 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 окремою графою за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів 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»).

Здобувач, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов'язаний перескласти її.

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**.

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

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 здобувачів, залікових книжках. ***Присутність здобувачів 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, 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 здобувачів, 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 (екзамен, залік) отримав незадовільну оцінку, складає його повторно. Повторне складання підсумкового екзамену чи заліку допускається не більше двох разів з кожної навчальної дисципліни: один раз – викладачеві, а другий – комісії, до складу якої входить керівник відповідної кафедри та 2-3 науково-педагогічних працівники.

Якщо дисципліна вивчається протягом двох і більше семестрів з семестровим контролем у формі екзамену чи заліку, то результат вивчення дисципліни в поточному семестрі визначається як середньоарифметичне значення балів, набраних у поточному та попередньому семестрах.

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

У цьому розділі також повинні бути розроблені чіткі критерії оцінювання здобувачів вищої освіти під час поточного контролю *(робота на семінарських, практичних, лабораторних та інших аудиторних заняттях, самостійна робота, виконання індивідуальних творчих завдань)* та підсумкового контролю. Кафедра визначає вимоги до здобувачів стосовно засвоєння змісту навчальної дисципліни, а саме: кількість оцінок, яку він повинен отримати під час аудиторної роботи, самостійної роботи. Наприклад:

Робота під час навчальних занять	**Самостійна та індивідуальна робота**	**Підсумковий контроль**
Отримати не менше 4 позитивних оцінок	Підготувати реферат, підготувати конспект за темою самостійної роботи, розв’язати задачі.	Отримати за підсумковий контроль не менше 30 балів

9. Шкала оцінювання: національна та ECTS

Оцінка в балах		Оцінка за національною шкалою	Оцінка за шкалою ECTS	
			Оцінка	Пояснення
12	97-100	Відмінно ("зараховано")	A	**"Відмінно"** – теоретичний зміст курсу освоєний **цілком,** необхідні практичні навички роботи з освоєним матеріалом сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані** в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
11	94-96			
10	90-93			
9	85 – 89	Добре ("зараховано")	B	**"Дуже добре"** – теоретичний зміст курсу освоєний **цілком**, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані**, якість виконання **більшості** з них оцінено числом балів, близьким до **максимального,** робота з двома – трьома незначними помилками.
8	80-84			
7	75 – 79		C	**"Добре"** – теоретичний зміст курсу освоєний **цілком**, практичні навички роботи з освоєним матеріалом **в основному** сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані**, якість виконання **жодного** з них **не оцінено мінімальним** числом балів, деякі види завдань виконані **з помилками,** робота з декількома незначними помилками, або з однією – двома значними помилками.
6	70 –74	Задовільно ("зараховано")	D	**"Задовільно"** – теоретичний зміст курсу освоєний **не повністю**, але **прогалини не носять істотного** характеру, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **більшість** передбачених програмою навчання навчальних завдань **виконано, деякі** з виконаних завдань, містять **помилки,** робота з трьома значними помилками.
5	65-69			
4	60 – 64		E	**"Достатньо"** – теоретичний зміст курсу освоєний **частково, деякі** практичні навички роботи **не сформовані, частина** передбачених програмою навчання навчальних завдань **не виконані,** або якість виконання деяких з них оцінено числом балів, близьким до **мінімального**, робота, що задовольняє мінімуму критеріїв оцінки.
3	40–59	Незадовільно ("не зараховано")	FX	**"Умовно незадовільно"** – теоретичний зміст курсу освоєний **частково**, необхідні практичні навички роботи **не сформовані, більшість** передбачених програм 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
2	21-40			
1	1–20		F	**"Безумовно незадовільно"** – теоретичний зміст курсу **не освоєно**, необхідні практичні навички роботи **не сформовані, всі виконані** навчальні завдання містять грубі **помилки, додаткова самостійна** робота над матеріалом курсу **не приведе** до значимого **підвищення якості** виконання навчальних завдань, робота, що потребує повної переробки

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

Основна

1. Програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
2. Робоча програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
3. Тулупов В.В. Вступ у спеціальність. Електронний курс лекцій. Харків, ХНУВС, 2020 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних занять з дисципліни " Вступ у спеціальність ". Харків, ХНУВС, 2020 р.
5. Олейніков А.М. Методи та засоби захисту інформації навчальний посібник / А. М. Олейніков. – Харків: НТМТ, 2014. - 298 с.
6. Юдін О.К., Богуш В.М. Інформаційна безпека держави. — Харків: Консум, 2012. — 576 с.
7. Носов, В.В., Манжай, А.В. Організація та забезпечення безпеки інформації навчальний посібник / В.В. Носов, А.В. Манжай. – Харків: ХНУВС, 2007. – 216 с., іл.
8. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
9. Рибальський О.В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України. К. : Вид. Національної академії внутріш. справ, 2012. 104 с.

Додаткова

10. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки / І. М. Рязанцева, В. В. Тулупов // Право і безпека. – 2014. –№ 2 (53). – С. 38-42
11. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.
12. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2018. 78 с.
13. Термінологічний довідник з питань технічного захисту інформації / ред. В. О. Хорошко. 3. вид., доп. і перероб. К. : ТОВ «Поліграф Консалтинг», 2003. 286 с.
14. Коженевський С. Р. Термінологічний довідник з питань технічного захисту інформації. Вид. 4-те, доп. і перероб. К. : ДУІКТ, 2007. 365 с.
15. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Нормативно-правові акти

16. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL:

https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
17. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15.
18. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
19. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
20. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
21. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
22. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.
23. Про ліцензування видів господарської діяльності : Закон України від 02.03.2015 № 222-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/222-19.
24. Про основні засади державного нагляду (контролю) у сфері господарської діяльності : Закон України від 05.04.2007 № 877-V // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/877-16.
25. Про акредитацію органів з оцінки відповідності : Закон України від 17.05.2001 № 2407-III // База даних «Законодавство України» / Верховна Рада України. URL https://zakon.rada.gov.ua/laws/show/2407-14:
26. Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання : Закон України від 20.02.2003 № 549-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/549-15.
27. Про наукову і науково-технічну експертизу : Закон України від 10.02.1995 № 51/95-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/51/95-%D0%B2%D1%80.
28. Про метрологію та метрологічну діяльність : Закон України від 05.06.2014 № 1314-VII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1314-18.
29. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
30. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 № 1229 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1229/99.
31. Про затвердження Концепції технічного захисту інформації в Україні : постанова Кабінету Міністрів України від 08.10.1997 № 1126 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF.

32. Про затвердження Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України : постанова Кабінету Міністрів України від 03.09.2014 № 411 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF.
33. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29.03.2006 № 373 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF.
34. Закон України «Про електронні довірчі послуги» від 05.10.2017 р. № 2155-VIII //Відомості Верховної Ради (ВВР), 2017, № 45, ст.400.
35. Про деякі питання захисту інформації, охорона якої забезпечується державою : постанова Кабінету Міністрів України від 13.03.2002 № 281 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/281-2002-%D0%BF.
36. Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації : постанова Кабінету Міністрів України від 04.02.1998 № 121 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/281-2002-%D0%BF.

Інформаційні ресурси в Інтернеті

37. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws.
38. Перелік нормативно-методичних документів в галузі захисту інформації // Облікові документи для секретного діловодства / ТОВ «НІКС» : офіційний веб сайт. URL: https://sites.google.com/a/nics.com.ua/price/.
39. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом // Державна служба спеціального зв’язку та захисту інформації України : офіційний веб сайт. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/category?cat_id=39181.
40. Відомості про засоби технічного захисту інформації, на які закінчився термін дії сертифікатів відповідності та експертних висновків // Державна служба спеціального зв’язку та захисту інформації України : офіційний вебсайт. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=234241&cat_id=39181.
41. Каталог обладнання для виявлення каналів витоку інформації // Digital and Analog Systems: офіційний вебсайт. URL: https://www.das-ua.com/katalog/obladnannya-dlya-viyavlennya-kanaliv-vitoku-informacii/.
42. Каталог обладнання для протидії засобам знімання інформації// Digital and Analog Systems: офіційний вебсайт. URL: https://www.das-ua.com/katalog/obladnannya-protidii-zasobam-znimannya-informacii/.