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
«___»_____ 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	першого (бакалаврського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем

2022 – 2023 навчальний рік

Розробник:

Рой Яніна Володимирівна, кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Рой Яніна Володимирівна, кандидат технічних наук, 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 _____ Павло СКЛАДАННИЙ

(підпис)

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.

Керівник освітньої програми _____ Артем ПЛАТОНЕНКО

(підпис)

Робочу програму перевірено

___.___. 2022 р.

Заступник декана _____ Євген ІВАНІЧЕНКО

(підпис)

Пролонговано:

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)

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

(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання		
	денна		заочна
«Методи та засоби управління інформаційною безпекою»			
Вид дисципліни	вибіркова		
Мова викладання, навчання та оцінювання	українська		
Загальний обсяг кредитів / годин	5 / 150		
Курс	3	4	
Семестр	6	7	
Кількість змістових модулів з розподілом:			
Обсяг кредитів	3	2	
Обсяг годин, в тому числі:	90	60	
Аудиторні	42	28	
Модульний контроль	6	4	
Семестровий контроль			
Самостійна робота	42	28	
Форма семестрового контролю	залік	залік	
Модуль 2			
Курс	4		-
Семестр	7		-
Кількість змістових модулів з розподілом:	2		
Обсяг кредитів	2		-
Обсяг годин, в тому числі:	60		-
Аудиторні	28		-
Модульний контроль	4		-
Семестровий контроль	-		-
Самостійна робота	28		-
Форма семестрового контролю	залік		-

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Методи та засоби управління інформаційною безпекою» 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, освітньої 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 першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Методи та засоби управління інформаційною безпекою» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Методи та засоби управління інформаційною безпекою» складається з двох змістових модулів: «Розробка та управління програмами інформаційної безпеки», «Управління інформаційними ризиками». Обсяг дисципліни – 60 год. (2 кредити).

Метою викладання навчальної дисципліни «Методи та засоби управління інформаційною безпекою» є формування у студентів уміння планувати, встановлювати та керувати здатністю виявляти, досліджувати, реагувати та відновлюватися після інцидентів інформаційної безпеки,

для мінімізації подальших впливів на структуру державних та комерційних структур.

Завдання полягає у формуванні теоретичних знань та практичних умінь у сфері управління інформаційної та кібернетичної безпеки і допоміжними процесами та набуття **наступних компетентностей**:

Фахові компетентності

КФ-3 — здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ-5 — здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації**.**

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен

знати:

- національну та міжнародну нормативно правову базу, науково-методичні та технічні принципи організації, впровадження та застосування систем управління захистом інформації в ІТС;
- організацію та порядок проведення робіт з проектування, впровадження та супроводу комплексних систем захисту інформації в інформаційних, комунікаційних та інформаційно – телекомунікаційних системах;
- вимоги міжнародних стандартів та вітчизняних нормативних документів в сфері захисту інформації щодо управління захистом інформації в інформаційних, комунікаційних та інформаційно – телекомунікаційних системах.
- вимоги міжнародних стандартів в галузі управління інформаційною безпекою;
- методи, методики, програмні засоби оцінки ризиків інформаційної безпеки в ІТС підприємств, установ, організацій.

уміти:

- здійснювати заходи щодо проектування, впровадження та супроводу, систем управління захистом інформації в інформаційних, комунікаційних та інформаційно – телекомунікаційних системах;
- застосовувати вимоги міжнародних стандартів та вітчизняних нормативних документів в сфері захисту інформації при проведенні оцінки стану захищеності ІТС та засобів захисту інформації, аудиту інформаційних систем та інформаційної безпеки.
- складати моделі загроз безпеки інформації та моделі потенційних порушників;

та досягти наступних **програмних результатів навчання:**

ПРз-8 — вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; проводити розслідування інцидентів інформаційної та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної та/або кібербезпеки; забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації.

ПРз-9 — володіти практичними навичками проведення аудиту безпеки ІКС, їх адміністрування та експлуатації; вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.

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	
Змістовий модуль 1. Розробка та управління програмами інформаційної безпеки							
Тема 1. Управління ресурсами програмами захисту інформації	15	2	4	2			7
Тема 2. Включення вимог безпеки інформації до контрактів, угод та зовнішніх управлінських процесів	15	2	2	4			7
Модульний контроль	2						
Разом	32	4	6	6			14
Змістовий модуль 2. Управління інформаційними ризиками							
Тема 3. Оцінювання доцільності та ефективності засобів контролю інформаційної безпеки	13	2	2	2			7
Тема 4. Організація ефективного повідомлення про інформаційний ризик	13	2	2	2			7
Модульний контроль	2						
Разом	28	4	4	4			14
Усього	60	8	10	10			28

5. Програма навчальної дисципліни

Змістовий модуль 1. Розробка та управління програмами інформаційної безпеки

Основні питання:

- Управління ресурсами програмами захисту інформації
- Включення вимог безпеки інформації до контрактів, угод та зовнішніх управлінських процесів
- Розробка та впровадження засобів захисту інформації
- Вирівнювання вимог програми захисту інформації згідно вимог інших функцій бізнес-структур

Змістовий модуль 2. Управління інформаційними ризиками

Основні питання:

- Оцінювання доцільності та ефективності засобів контролю інформаційної безпеки
- Організація ефективного повідомлення про інформаційний ризик
- Визначення, оцінка та реагування на ризик відповідним способом

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної 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

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	2	2	2	2
Відвідування семінарських занять	1	3	3	2	2
Відвідування практичних занять	1	3	3	2	2
Відвідування лабораторних занять	1				
Робота на семінарському занятті	10	3	30	2	20
Робота на практичному занятті	10	3	30	2	20
Лабораторна робота (в тому числі допуск, виконання, захист)	10				
Виконання завдань для самостійної роботи	5	1	5	1	5
Виконання модульної роботи	25	2	25	1	25
Виконання ІНДЗ	30				
Разом		-	98	-	76
Максимальна кількість балів: 174					
Розрахунок коефіцієнта: 174/100=1,74					

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. Розробка та управління програмами інформаційної безпеки		14	5
1	Вирівнювання вимог програми захисту інформації згідно вимог інших функцій бізнес-структур: • виконання завдань відповідно до теми; • опрацювання фахових видань.	14	5
Змістовий модуль 2. Управління інформаційними ризиками		14	5
2	Визначення, оцінка та реагування на ризик відповідним способом: • виконання завдань відповідно до теми; • опрацювання фахових видань.	14	5
Разом		28	10

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 з комплексних запитань.

Модульна контрольна робота оцінюється у 35 балів.

Форми проведення семестрового контролю та критерії оцінювання

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

Орієнтовний перелік питань для самоконтролю

1. Концептуальні засади забезпечення інформаційної безпеки України.
2. Нормативно-правові основи захисту інформації в Україні.
3. Концепція національної безпеки України, концепція інформаційної безпеки України.
4. Доктрина інформаційної безпеки України.
5. Доктрини інформаційної безпеки країн ЄС.
6. Доктрини інформаційної безпеки США.
7. Місце технічного захисту інформації у системі інформаційної безпеки.
8. Сутність та завдання технічного захисту інформації.
9. Способи несанкціонованого зняття інформації.
10. Визначення можливих джерел витоку акустичної та електромагнітної інформації у приміщенні.
11. Визначення можливих джерел витоку інформації з радіоканалу.
12. Складові ТЗІ.
13. Методи пасивного та активного захисту інформації.
14. Методи та засоби захисту акустичної інформації.
15. Методи та засіб захисту електромагнітної інформації.
16. Методи захисту від ВЧ-нав'язування.
17. Методики і засоби пошуку радіозакладних пристроїв.
18. Методи захисту інформації у автоматизованих системах.
19. Програмні засоби захисту інформації.
20. Вибір програм розмежування доступу до інформації.
21. Вибір та застосування антивірусних програм.
22. Вибір програм автоматичного шифрування інформації при її збереженні на дисках та відпрацювання практичних навичок їх застосування.
23. Методи захисту інформації у телекомунікаційних мережах та відкритих мережах зв'язку.
24. Захист мовленнєвої інформації, що передається у відкритих каналах зв'язку.

25. Загальні принципи побудови захищених інформаційно-комунікаційних систем (ЗІКС) та КМ.
26. Призначення та класифікація ІКМ та КМ.
27. Логічна та фізична структури ІКМ та КМ.
28. Телекомунікаційна система КМ та характеристика її елементів.
29. Завдання адміністрування та експлуатація захищених інформаційно-комунікаційних систем.
30. Атестацію захищених інформаційних та комунікаційних систем в умовах додержання режиму секретності із зафіксуванням результатів у відповідних документах.
31. Основні принципи організації взаємодії в ЗІКС та КМ.
32. Логічна модель взаємодії ЗІКС та КМ.
33. Функціональні рівні взаємодії та їх ієрархія.
34. Особливості еталонної моделі взаємодії відкритих систем (ВВС) для локальних комп'ютерних мереж (ЛКМ).
35. Програмне забезпечення для адміністрування ЗІКС та КМ.
36. Структура, призначення, склад і загальна характеристика основних елементів.
37. Мережеві операційні системи та їх характеристика.
38. Аналізатори протоколів.
39. Особливості функціонування ОС різних типів.
40. Основи мережевої безпеки.
41. Адміністрування у ОС NetWare фірми Novell.
42. Засоби управління локальними ресурсами ЗІКС та КМ.
43. Якісний та кількісний аналіз ризику для ІБ та КБ об'єкту інформатизації.
44. Сутність якісного та кількісного аналізу ризиків для ІБ та кібербезпеки підприємства, фірми.
45. Принципи аналізу ризиків для ІБ.
46. Напрямки аналізу підприємницьких ризиків для ІБ.
47. Збитки, які виникають в процесі підприємницької діяльності.
48. Методи аналізу ступеня ризику для ІБ.
49. Характеристика області абсолютної стійкості, нормальної стійкості, області нестійкого стану, критичного стану, кризового стану підприємства на основі аналізу ризику для ІБ.
50. Методи кількісної оцінки ступеня ризику: аналітичний метод; метод використання аналогів. Комплексна оцінка ризиків для ІБ.
51. Визначення ключового параметру, вибір чинників впливу, програмування величини ключового параметру для оцінки ризиків ІБ та КБ.
52. Визначення імовірності досліджуваного проекту на основі оцінок імовірності проектів-аналогів для побудови СЗІ на ОБІ.
53. Прогноз очікуваних характеристик досліджуваного проекту захисту ОБІ.
54. Принципи управління ризиками ІБ.
55. Система управління ризиками ІБ.
56. Основи профілактики ризиків: диверсифікація та лімітування.
57. Ризики, пов'язані з вкладенням капіталу у засоби ЗІ.
58. Комплексне управління довгостроковими інвестиціями у політику ІБ ОБІ.

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: 60 год., лекції – 8 год., практичні заняття – 10 год., лабораторні роботи – 10 год., модульний контроль – 4 год., самостійна робота – 28 год.

Модулі (назви, бали)	**Змістовий модуль 1. Розробка та управління програмами інформаційної безпеки (98 балів)**		**Змістовий модуль 2. Управління інформаційними ризиками (76 балів)**	
Лекції (теми, бали)	Управління ресурсами програмами захисту інформації (1 бал)	Включення вимог безпеки інформації до контрактів, угод та зовнішніх управлінських процесів (1 бал)	Оцінювання доцільності та ефективності засобів контролю інформаційної безпеки (1 бал)	Організація ефективного повідомлення про інформаційний ризик (1 бал)
Семінарські заняття (теми, бали)	Міжнародні та вітчизняні стандарти в галузі управління, оцінки та аудиту інформаційної безпеки (22 бали)	Побудова підсистеми інформаційної безпеки (11 балів)	Методи оцінки ризиків інформаційної безпеки. Оцінка інформаційних ризиків з використання методів системного аналізу (11 балів)	Організаційна структура системи забезпечення безпеки інформації (11 балів)
Практичні заняття (теми, бали)	Дослідження атак з допомогою штучно занесених програм класу SpyWare. (11 балів)	Мереживі сканери та екрани (22 бали)	Огляд методів та засобів захисту інформації (11 балів)	Огляд складових інформаційної безпеки (11 балів)
Самостійна робота	Самостійна робота (5 балів)		Самостійна робота (5 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)		Модульна контрольна робота 2 (25 балів)	
Підсумковий контроль (вид, бали)	залік			

8. Рекомендовані джерела

Основна (базова):

1. Єсін В.І., Кузнєцов А.А., Сорока Л.С. Безпека інформаційних систем та технологій – Х.: «ЕДЕНА», 2010. – 656с.
2. Горбенко І.Д., Гриненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації – Харків: ХНУРЕ, 2004 – 368 с.
3. Домарев В.В. Безпека інформаційних технологій: Системний підхід. – К.: "ТІД ДС", 2004. – 992с.

Додаткова

1. Білов Є.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основи інформаційної безпеки: Навч. посібник для ВНЗ. – Львів: Видавництво «Ранок», 2006. – 544 с.
2. Завгородній В.І. Комплексний захист інформації в комп’ютерних системах: Навч. посібник. - К.: Логос, 2011. – 264 с.
3. Хорошков В.К., Чекатков А.А. Методи и засоби захисту інформації / За ред. Ю.С. Ковтанюка – К.: Видавництво «Юніор», 2013. – 504с.
4. Zachman John A., «Enterprise Architecture: The Past and the Future» Article published in DM Review Magazine. December 1999 Issue.

9. Додаткові ресурси (інформаційні ресурси)

1. The Zachman Framework™: A Concise Definition, http://zachmaninternational.com.
2. Introducing The Open Group Architecture Framework (TOGAF), http://www.ibm.com.
3. Service-Oriented Architecture and Enterprise Architecture, http://www.ibm.com.
4. Microsoft Operations Framework; Cross Reference ITIL v3 and MOF 4.0. Microsoft Corporation. May 2009. http://go.microsoft.com/fwlink/?LinkId=151991.