Прим. № 1

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Системи управління інформаційною безпекою»

Освітня програма	*Кіберзахист інформаційних ресурсів*
Рівень вищої освіти	*перший (бакалаврський)*
Форма навчання	*денна*
Статус навчальної дисципліни	*обов'язкова*
Мова викладання	*українська*

КИЇВ – 2024

N406 ПО ОК 417

Робочу програму навчальної дисципліни розглянуто та схвалено на засіданні кафедри технічного захисту інформації від 18.09.2024 року, протокол № 12.

1. Опис навчальної дисципліни

Показник	Значення показника
Курс	3
Семестр	6
Обсяг *(кредити ЄКТС/години)*	5 / 150
Кількість змістових модулів	3
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	18
семінарські заняття (СЗ)	38
самостійна робота (СР)	94
форма підсумкового контролю	*Екзамен (6)* *Курсова робота (6)*

Передумовами для вивчення та успішного засвоєння навчальної дисципліни «Системи управління інформаційною безпекою» є: «Системний аналіз та прийняття рішень в інформаційній сфері», «Інформаційна безпека», «Проектування та безпека баз даних».

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

Мета: Набуття студентами знань, умінь і навичок необхідних для вироблення рішень щодо ефективного функціонування системи управління інформаційною безпекою у різних сферах професійної діяльності.

Завдання: Завданням вивчення дисципліни «Системи управління інформаційною безпекою» є: засвоєння студентами основних принципів та інструментарію щодо постановки задач, основних методів їх розв'язування та аналізу, придбання практичних навичок для вибору оптимальної методики побудови та функціонування системи управління інформаційною безпекою

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Системи управління інформаційною безпекою» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної програми «Кіберзахист інформаційних ресурсів» *(від* 11.09.2024 *№29/3/1/3-1277ві)*, а саме:

ПРН-03. Застосовувати результати алгоритмічного та абстрактного мислення, самостійного пошуку, аналізу та синтезу, методів теорії інформації, теорії систем та системного аналізу для ефективного вирішення завдань професійної діяльності, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.

ПРН-07. Обґрунтовувати та визначати основні напрями створення та експлуатації системи та основних підсистем управління інформаційною безпекою та кібербезпекою, використовуючи інформаційні та комунікаційні технології для формування ефективної системи інформаційно-аналітичного забезпечення, підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.

ПРН-09. Вміти здійснювати комплексний аналіз загроз національній безпеці, розробляти та реалізовувати ефективні стратегії їх нейтралізації, застосовуючи знання з основ теорії національної безпеки та синтезуючи різнопланову інформацію.

ПРН-13. Оцінювати стан безпеки особистості, суспільства та держави за окремими сферами забезпечення і видами діяльності на основі положень теорії безпеки окремих сфер забезпечення національної безпеки і видів діяльності.

ПРН-19. Демонструвати здатність розробляти та впроваджувати комплексні стратегії управління інформаційною та кібербезпекою на різних рівнях, що охоплюють окремі організації, державні і міжнародні структури, спираючись на глибоке розуміння теоретичних основ та застосовуючи набуті практичні навички аналізу, дослідження та підготовки відповідної документації.

ПРН-24. Забезпечувати процеси захисту та функціонування інформаційно-комунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

3. Програма та структура навчальної дисципліни

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Змістовий модуль 1. Методологічні основи і підходи до впровадження системи управління інформаційною безпекою.						
Тема 1. Методологічні основи та підходи до управління безпекою організації.	**8**	**2**	**2**			**4**
Лекція 1. Методологічні основи та підходи до управління безпекою організації.		2				
Спмінарське заняття 1. Методологічні основи та підходи до управління безпекою організації.			2			
Самостійна робота 1. За матеріалами Теми 1						4
Тема 2. Основи створення та впровадження системи інформаційної безпеки.	**8**	**2**	**2**			**4**
Лекція 2. Основи створення та впровадження системи інформаційної безпеки		2				
Спмінарське заняття 2. Основи створення та впровадження системи інформаційної безпеки.			2			
Самостійна робота 2. За матеріалами Теми 2						4
Тема 3. Особливості побудови ефективної системи управління інформаційною безпекою.	**8**	**2**	**2**			**4**
Лекція 3. Особливості побудови ефективної системи управління інформаційною безпекою.		2				
Семінарське заняття 3. Створення та функціонування системи управління інформаційною безпекою..			2			
Самостійна робота 3. За матеріалами Теми 3						4
Тема 4. Інформаційні загрози та вразливості, як складові ризиків інформаційної безпеки.	**8**		**2**			**6**
Семінарське заняття 4. Інформаційні загрози та вразливості, як складові ризиків інформаційної безпеки.			2			
Самостійна робота 4. За матеріалами Теми 4						6
Тема 5. Підхід до управління інформаційною безпекою на основі управління ризиками.	**8**		**2**			**6**
Семінарське заняття 5. Управління інформаційною безпекою на основі управління ризиками.			2			
Самостійна робота 5. За матеріалами Теми 5.						6
Тема 6. Методи обстеження ІС по виявленню загроз та вразливостей.	**8**		**4**			**4**

Семінарське заняття 6. Методи обстеження ІС по виявленню загроз та вразливостей.			2			
Самостійна робота 6. За матеріалами Теми 6.						4
Семінарське заняття 7. **Модульна контрольна робота 1**			2			
Всього годин за змістовий модуль 1	**48**	**6**	**14**			**28**
Змістовий модуль 2. Управління ризиками та інцидентами інформаційної безпеки як основа системи управління інформаційною безпекою.						
Тема 7. Модель системи управління інформаційною безпекою відповідно до ДСТУ ISO/IEC 27005:2023 (Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки).	**10**	**2**				**8**
Лекція 4. Модель системи управління інформаційною безпекою відповідно до ДСТУ ISO/IEC 27005.		2				
Самостійна робота 7. За матеріалами Теми 7.						8
Тема 8. Процес менеджменту ризиків інформаційної безпеки.	**10**	**2**	**2**			**6**
Лекція 5. Процес менеджменту ризиків інформаційної безпеки.		2				
Семінарське заняття 8. Менеджменту ризиків інформаційної безпеки			2			
Самостійна робота 8. За матеріалами Теми 8.						6
Тема 9. Організаційна структура управління ризиками та прийняття управлінських рішень.	**10**		**2**			**8**
Семінарське заняття 9. Організаційна структура управління ризиками та прийняття управлінських рішень. .			2			
Самостійна робота 9. За матеріалами Теми 9.						8
Тема 10. Побудова системи управління ризиками інформаційної безпеки на на об'єктах інформаційної діяльності.	**10**		**2**			**8**
Семінарське заняття 10. Побудова системи управління ризиками інформаційної безпеки на об'єктах інформаційної діяльності**.** .			2			
Самостійна робота 10. За матеріалами Теми 10.						8
Тема 11. Управління інцидентами в процесі розвитку та функціонування СУІБ.	**10**	**2**	**4**			**4**
Лекція 6. Управління інцидентами в процесі розвитку та функціонування СУІБ		2				
Семінарське заняття 11. Управління інцидентами в процесі розвитку та функціонування СУІБ			2			
Самостійна робота 11. За матеріалами Теми 11.						4
Семінарське заняття 12. **Модульна контрольна робота 2**			2			
Всього годин за змістовий модуль 2	**50**	**6**	**10**			**34**
Змістовий модуль 3. Створення, впровадження та функціонування систем управління інцидентами та безперервності бізнесу в сфері управління інформаційною безпекою.						
Тема 12. Виявлення і оброблення подій та інцидентів інформаційної безпеки.	**8**	**2**	**2**			**4**
Лекція 7. Виявлення і оброблення подій та інцидентів інформаційної безпеки.		2				

Семінарське заняття 13. Виявлення і оброблення подій та інцидентів інформаційної безпеки.			2			
Самостійна робота 12. За матеріалами Теми 12						4
Тема 13. Реагування на інциденти інформаційної безпеки.	**8**		**2**			**6**
Семінарське заняття14. Реагування на інциденти інформаційної безпеки.			2			
Самостійна робота 13. За матеріалами Теми 13.						6
Тема 14. Система управління інцидентами інформаційної безпеки.	**8**	**2**	**2**			**4**
Лекція 8. Система управління інцидентами інформаційної безпеки.		2				
Семінарське заняття15. Система управління інцидентами інформаційної безпеки.			2			
Самостійна робота 14. За матеріалами Теми 14.						4
Тема 15. Функціонування системи управління інцидентами інформаційної безпеки.	**8**		**2**			**6**
Семінарське заняття16. Функціонування системи управління інцидентами інформаційної безпеки.			2			
Самостійна робота 15. За матеріалами Теми 15.						6
Тема 16. Система управління безперервністю бізнесу	**6**	**2**				**4**
Лекція 9. Система управління безперервністю бізнесу		2				
Самостійна робота 16. За матеріалами Теми 16.						4
Тема 17. Життєвий цикл управління безперервністю бізнесу.	**6**		**2**			**4**
Семінарське заняття17. **Життєвий цикл управління безперервністю бізнесу**.			2			
Самостійна робота 17. За матеріалами Теми 17.						4
Тема 18. Забезпечення безперервності бізнесу.	**8**		**4**			**4**
Семінарське заняття17. **Забезпечення безперервності бізнесу.**			2			
Самостійна робота 18. За матеріалами Теми 18.						4
Семінарське заняття19. **Модульний контроль 3.**			2			
Всього годин за змістовий модуль 3	**52**	**6**	**14**			**32**
Підсумковий контроль *(форма)* *Екзамен*						
Всього годин за навчальну дисципліну	**150**	**18**	**38**			**94**

4. Основні методи навчання

Під час викладання курсу передбачено застосування таких методів як навчальна лекція, лекція-діалог, семінар, бесіда, а також наочних методів навчання, зокрема використання мультимедійних засобів, показ слайдів та презентацій. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.

5. Оцінювання результатів навчання

5.1 Результати навчання здобувача вищої освіти з навчальної дисципліни оцінюються за 100-бальною шкалою як сума балів поточного та підсумкового

контролю із застосуванням наступних вагових коефіцієнтів, загальна сума яких дорівнює 1:

Вид контролю	Ваговий коефіцієнт
Поточний контроль (К)	0,2
Курсова робота (КР)	0,4
Підсумковий контроль (ПК)	0,4

Підсумкова семестрова оцінка (ПСО) обчислюється за формулою: ПСО=К+КР+ПК

5.2. Складниками для обчислення балу поточного контролю здобувача вищої освіти є:

Види навчальної діяльності	Кількість балів (максимальна)
Робота на лекціях (ведення конспекту лекцій або інше)	20
Робота на семінарських заняттях	20
Робота на практичних заняттях	-
Робота на лабораторних заняттях	-
Виконання завдань для самостійної роботи	20
Виконання індивідуальних та/або групових завдань	-
Виконання курсової роботи	40

Мінімальна кількість балів для допуску до підсумкового контролю - 60

5.3. Шкала оцінювання здобувача вищої освіти

Оцінка за шкалою ЄКТС	Оцінка за 100-бальною шкалою	Значення оцінки
A	90-100	*Відмінно – відмінне виконання лише з незначною кількістю помилок.* Здобувач вищої освіти виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили.
B	84-89	*Дуже добре – вище середнього рівня, але з кількома помилками.* Здобувач вищої освіти вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв'язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна.
C	75-83	*Добре – загалом правильна робота, але з певною кількістю помилок.* Здобувач вищої освіти вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок.
D	65-74	*Задовільно – непогано, але зі значною кількістю недоліків.* Здобувач вищої освіти відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих.
E	60-64	*Достатньо – виконання задовольняє мінімальні вимоги.* Здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.
FX	35-59	*Незадовільно – потрібна додаткова робота.* Здобувач вищої освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу
F	1-34	*Незадовільно – потрібна значна додаткова робота.* Здобувач вищої освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів.

6. Ресурсне забезпечення навчальної дисципліни

Рекомендовані джерела інформації

Основна література:

1. Управління інформаційною безпекою та кібербезпекою організації: Навч. посіб. в 2 ч. Ч. 1: Основи менеджменту інформаційної безпеки та кібербезпеки / В. М. Богуш, В. Д. Бровко, С. Б. Гордієнко, В. Д. Козюра, А. М. Кудін. Київ: НА СБУ, 2023. - 168 с.
2. Управління інформаційною безпекою та кібербезпекою організації: Навч. посіб. в 2 ч. Ч. 2: Основи побудови системи і основних підсистем управління інформаційною безпекою та кібербезпекою організації / В. М. Богуш, В. Д. Бровко, С. Б. Гордієнко, В. Д. Козюра, А. М. Кудін. Київ: НА СБУ, 2023. - 208 с.
3. Домарєв В. В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) / В. В. Домарєв, В. В. Домарєв. – Донецьк: Велстар, 2012, 2012 – 146 с.
4. Гордієнко С.Б. Актуальні питання управління IT ризиками на об'єктах критичної інформаційної інфраструктури // Вісник Державного університету телекомунікацій «Телекомунікаційні та інформаційні технології» №1 (74) - 2022. – С.29-35.
5. ДСТУ ISO/IEC 27000:2023. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT).
6. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)
7. ДСТУ ISO/IEC 27002:2023. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).
8. ДСТУ ISO/IEC 27005:2023. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT).
9. ДСТУ ISO/IEC 27006:2023. Інформаційні технології. Методи захисту. Вимоги до організацій, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою (ISO/IEC 27006:2011, IDT).
10. Гладиш С. В., Кононович В. Г., Тардаскін М. Ф. Розподіл відповідальності щодо реагування та обробки інцидентів безпеки в інформаційно-телекомунікаційній мережі загального користування // Зв'язок. — 2007. — № 8. — С. 28–31.
11. Безперервність бізнесу // Банківська енциклопедія / С. Г. Арбузов, Ю. В. Колобов, В. І. Міщенко, С. В. Науменкова. — Київ : Центр наукових досліджень Національного банку України : Знання, 2011. — 504 с. — (Інституційні засади розвитку банківської системи України).

29/3/1/4 - 1488/БІ
14. 10. 2024