Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з наукової роботи
Наталія ВІННІКОВА
«01» вересня 2022р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВЕДЕННЯ КІБЕРДІЙ І КІБЕРКОНФЛІКТІВ

для аспірантів

спеціальності 125 Кібербезпека

освітньо рівня третього (освітньо-наукового)

освітньо-наукової програми «Інформаційна безпека держави»

Київ – 2022

Розробник:

Аносов Андрій Олександрович, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та управління

Викладач:

Аносов Андрій Олександрович, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та управління

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

Протокол від 08.09.2021 №10

Завідувач кафедри _____ Павло СКЛАДАННИЙ
(підпис)

Робочу програму погоджено з гарантом освітньо-наукової програми «Інформаційна безпека держави**»**
08.09.2021

Гарант освітньо-наукової програми _____ Наталія КОРШУН
(підпис)

Робочу програму перевірено
09.09.2021

Завідувач аспірантури, докторантури _____ Ілона ТРИГУБ
(підпис)

Пролонговано:

на 2022/2023 н.р. _____ (_____), «01» 09 2022 р., протокол № 12
(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 № ___

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	вибіркова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4/120	
Рік навчання	3	3
Семестр	6	6
Кількість змістових модулів з розподілом:	4	
Обсяг кредитів	4	4
Обсяг годин, в тому числі:	120	120
Аудиторні	32	16
Модульний контроль	8	-
Семестровий контроль	30	30
Самостійна робота	50	74
Семестровий контроль	Іспит	

2. Мета та завдання навчальної дисципліни

Мета: формування в аспірантів знань, умінь і навичок з застосування теоретичних основ та впровадження технологій забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів.

Завдання: отримання теоретичних знань та практичних умінь з дослідження теорій і технологій забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів:

– здатність застосовувати сучасні інформаційні та безнекові технології (комплексні системи криптографічного і технічного захисту інформації, системи соціотехнічної безпеки тощо);

– здатність до планування і реалізації заходів із захисту інформації на об'єктах критичної інфраструктури;

– здатність проводити моніторинг, аудит та відновлення процесів штатного функціонування ІТ систем та мереж на об'єктах критичної інфраструктури після збоїв та відмов різних класів і походження.

У результаті вивчення навчальної дисципліни відповідно до освітньо-наукової програми спеціальності формуються фахові компетентності:

Програмні компетентності	**Код**	**Значення компетентності**
Фахові компетентності (КФ)	**ФК-4**	Здатність проектувати, впроваджувати і застосовувати сучасні інформаційні та безпекові технології (комплексні системи криптографічного і технічного захисту інформації, системи соціотехнічної безпеки тощо)
	ФК-7	Здатність до планування і реалізації заходів із захисту інформації на об'єктах критичної інфраструктури, проведення моніторингу, аудиту та відновлення процесів штатного функціонування ІТ систем та мереж після збоїв та відмов різних класів і походження.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни аспірант повинен

знати:

– системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів;

– науково-організаційні основи проведення аудиту безпеки ІКС, а також наукові методи щодо створення систем моніторингу безпеки в ІТ системах та мережах;

– сучасні методи проведення наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД.

вміти:

– застосовувати сучасні інформаційно-комунікаційні технології як в побуті, так і в професійній діяльності;

– проводити проведенням наукових і науково- технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД;

– обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах;

– використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об’єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.

та досягти наступних програмних результатів навчання:

– вирішувати задачі керування проведенням наукових і науково- технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД;

– вирішувати задачі централізованого і децентралізованого адміністрування доступом до ІР і процесів в ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них;

– вирішувати задачі централізованого і децентралізованого адміністрування доступом до ІР і процесів в ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них.

Програмні результати навчання:

Код	Значення програмного результату
ПРН-4	- забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів; - здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності; - проводити або керувати проведенням наукових і науково- технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД; - обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах; - використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об’єктів інформаційної діяльності, а також наукових досліджень вищих рівнів;

ПРН-7	- вирішувати задачі централізованого і децентралізованого адміністрування доступом до ІР і процесів в ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них; - володіти науково-організаційними основами проведення аудиту безпеки ІКС, а також науковими методами та практичними навичками щодо створення систем моніторингу безпеки в ГГ системах та мережах.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назви змістових модулів і тем	Усього	Розподіл годин між видами робіт			
		Аудиторна			Самостійна
		Лекції	Семінарські	Практичні	
Змістовий модуль І. Тенденції розвитку і застосування методів і засобів захисту інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів					
Тема 1. Тенденції розвитку і застосування методів і засобів захисту інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів	24	4	4	1	15
Модульний контроль	2				
Разом	**26**	**4**	**4**	**1**	**15**
Змістовий модуль ІІ. Проблеми захисту державної інформаційної сфери від стороннього кібернетичного впливу					
Тема 2. Проблеми захисту державної інформаційної сфери від стороннього кібернетичного впливу	24	4	4	1	15
Модульний контроль	2				
Разом	**26**	**4**	**4**	**1**	**15**
Змістовий модуль ІІІ. Технології та інструменти забезпечення безпеки інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів.					
Тема 3. Технології та інструменти забезпечення безпеки інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів.	19	4	4	1	10
Модульний контроль	2				
Разом	**21**	**4**	**4**	**1**	**10**
Змістовий модуль ІV. Технології адміністрування та експлуатації об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів					
Тема 4. Технології адміністрування та експлуатації об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів	15	2	2	1	10
Модульний контроль	2				
Разом	**17**	**2**	**2**	**1**	**10**
Семестровий контроль	**30**				
Усього	**120**	**14**	**14**	**4**	**50**

Тематичний план для заочної форми навчання

Назви змістових модулів і тем	Усього	Розподіл годин між видами робіт			
		Аудиторна			Самостійна
		Лекції	Семінарські	Практичні	
Змістовий модуль І Тенденції розвитку і застосування методів і засобів захисту інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів					
Тема 1. Тенденції розвитку і застосування методів і засобів захисту інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів	24	2	2		20
Разом	**24**	**2**	**2**		**20**
Змістовий модуль ІІ. Проблеми захисту державної інформаційної сфери від стороннього кібернетичного впливу					
Тема 2. Проблеми захисту державної інформаційної сфери від стороннього кібернетичного впливу	24	2		2	20
Разом	**24**	**2**		**2**	**20**
Змістовий модуль ІІІ. Технології та інструменти забезпечення безпеки інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів.					
Тема 3. Технології та інструменти забезпечення безпеки інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів..	24	2	2		20
Разом за змістовим модулем	**24**	**2**	**2**		**20**
Змістовий модуль ІV Технології адміністрування та експлуатації об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів					
Тема 4. Технології адміністрування та експлуатації об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів	18		2	2	14
Разом	**18**	**2**	**2**	**2**	**14**
Семестровий контроль	**30**				
Усього	**120**	**6**	**6**	**4**	**74**

5. Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ І. Тенденції розвитку і застосування методів і засобів захисту інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів

Тема 1. Тенденції розвитку і застосування методів і засобів захисту інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів

Тенденції розвитку і застосування методів і засобів захисту інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів. Тенденції розвитку методів і засобів захисту інформації. Тенденції побудови архітектури безпеки інформації. Захист інформації в корпоративних мережах. Основи і мета політики безпеки в корпоративних мережах. Принципи та методи надання доступу до інформаційних ресурсів. Принципи забезпечення доступу до інформаційних ресурсів. Методи ідентифікації і аутентифікації користувачів. Методи контролю доступу. Профіль безпеки стандарту ISO/IEC 15408.

Ключові слова: захищені ОІД, методологія захисту інформації на ОІД, методи захисту інформації на ОІД, проектування систем захисту, проектування захищених інформаційних систем.

ЗМІСТОВИЙ МОДУЛЬ ІІ. Проблеми захисту державної інформаційної сфери від стороннього кібернетичного впливу

Тема 2. Проблеми захисту державної інформаційної сфери від стороннього кібернетичного впливу

Основні суб'єкти державної інформаційної інфраструктури. Завдвння та функції суб'єктів державної інформаційної інфраструктури. Моделювання стратегій захисту інформації від стороннього кібернетичного впливу. Визначення переліку суб'єктів і встановлення ідентифікаторів. Встановлення повноважень і прав суб'єктів щодо об'єктів. Питання своєчасного виявлення та адекватного реагування на інциденти інформаційної безпеки. Завдання своєчасного виявлення інцидентів інформаційної безпеки. Перспективні напрямки державної політики у галузі кібернетичної безпеки.

Ключові слова: аналіз захищеності ОІД, технологічна модель, технологічна модель захисту ОІД, концепція захисту інформації на ОІД, забезпечення інформаційної безпеки, інструменти забезпечення безпеки інформації.

ЗМІСТОВИЙ МОДУЛЬ ІІІ. Технології та інструменти забезпечення безпеки інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів.

Тема 3. Технології та інструменти забезпечення безпеки інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів.

Технологічна модель забезпечення безпеки інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів. Технології захисту інформації в системах інформаційної та/або кібербезпеки.

Концепція захисту інформації, організації й забезпечення інформаційної та кібербезпеки ОІД.

Ключові слова: концепція захисту інформації, технологічна модель, алгоритми захисту, моделі захисту, методи захисту, програмні комплекси кібербезпеки ОІД.

ЗМІСТОВИЙ МОДУЛЬ IV. Технології адміністрування та експлуатації об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів

Тема 4. Технології адміністрування та експлуатації об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів

Адміністрування процесів введення в експлуатацію та експлуатації об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів. Перевірка і підтримка цілісності даних на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів. Розмежування прав доступу та правила забезпечення безпеки даних на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів. Удосконалення, модернізація та уніфікація систем, засобів і технологій забезпечення безпеки на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів.

Ключові слова: об'єкт критичної інфраструктури, ведення кібердій і кіберконфліктів, адміністрування, експлуатація, адміністрування захищених систем, експлуатація захищених систем, права доступу, правила забезпечення безпеки, цілісність даних.

Ключові слова: теорія ігор, марковські процеси, мережа Петрі, нечіткі множини.

6. Контроль навчальних досягнень

6.1. Система оцінювання навчальних досягнень аспірантів денної форми навчання

№ з/п	Вид діяльності аспіранта	Макс. кільк. балів заолинишю	Модуль 1		Модуль 2		Модуль 3		Модуль 4	
			Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів
1	Відвідування лекцій	1	3	3	3	3	3	3	3	3
2	Відвідування практичних занять	1	4	4	4	4	4	4	4	4
3	Відвідування семінарських занять									
4	Робота на практичних заняттях	10	4	40	4	40	4	40	4	40
5	Робота на семінарських заняттях									
4	Виконання завдань для самостійної роботи	5	3	15	3	15	3	15	3	15
5	Виконання модульної контрольної роботи	25	1	25	1	25	1	25	1	25

№ з/п	Вид діяльності аспіранта	Макс. кільк. балів заолинишю	Модуль 1		Модуль 2		Модуль 3		Модуль 4	
			Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів
6	Макс. кількість балів за видами поточного контролю			**87**		**87**		**87**		**87**
7	Максимальна кількість балів:	**348**								
8	Розрахунок коефіцієнта Бал max / Сума балів max	**60/348=0,17**								

Система оцінювання навчальних досягнень аспірантів заочної форми навчання

№ з/п	Вид діяльності аспіранта	Макс. кільк. балів заолинишю	Модуль 1		Модуль 2		Модуль 3		Модуль 4	
			Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів	Кільк.один.	Кільк.один.	Макс. кільк. балів	Кільк.один.
1	Відвідування лекцій	1	1	1	1	1	1	1		
2	Відвідування практичних занять	1	1	1	1	1	1	1	2	2
3	Відвідування семінарських занять									
4	Робота на практичних заняттях	10	1	10	1	10	1	10	2	20
5	Робота на семінарських заняттях									
4	Виконання завдань для самостійної роботи	5	6	30	6	30	6	30	6	30
6	Макс. кількість балів за видами поточного контролю			**42**		**42**		**42**		**52**
7	Максимальна кількість балів:	**178**								
9	Розрахунок коефіцієнта Бал max / Сума балів max	**60/178=0,34**								

Умовою зарахування кожного змістовного модулю та отримання аспірантом заліку є здобуття не менше 35% балів (Бал min / Бал max = 35:100=0,35) за результатами всіх видів означених діяльностей в кожному змістовному модулі.

6.2. Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом позааудиторної індивідуальної діяльності аспіранта, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності. В межах кожної теми аспіранти, використовуючи рекомендовану літературу, повинні самостійно опрацювати джерела за запропонованою тематикою. Завдання для самостійної роботи подаються письмово. Кожна робота оцінюється від 1-5 балів.

Перелік тем для самостійної роботи аспірантів очної форми навчання

№ з/п	Назва теми
Змістовий модуль 1. Тенденції розвитку і застосування методів і засобів захисту інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів	
1	Тенденції розвитку методів і засобів ведення кібердій і кіберконфліктів
2	Застосування методів і засобів захисту інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів
3	Основні методології проектування систем захисту інформації на об'єктах критичної інфраструктури
Змістовий модуль 2. Проблеми захисту державної інформаційної сфери від стороннього кібернетичного впливу	
4	Проблеми захисту державної інформаційної сфери від стороннього кібернетичного впливу
5	Забезпечення інформаційної безпеки державної інформаційної сфери від стороннього кібернетичного впливу
6	Алгоритми, моделі, методи оцінки характеристик і стану систем інформаційної та кібербезпеки державної інформаційної сфери
Змістовий модуль 3. Технології та інструменти забезпечення безпеки інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів	
7	Технології забезпечення безпеки інформації в системах і мережах
8	Технологічна модель безпеки інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів
9	Концепція захисту інформації, організації й забезпечення інформаційної та кібербезпеки ОІД.
Змістовий модуль 4. Технології адміністрування та експлуатації об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів	
10	Адміністрування процесів введення в експлуатацію захищених ІТ систем і мереж
11	Адміністрування процесів експлуатації захищених ІТ систем і мереж
12	Удосконалення систем, засобів і технологій забезпечення безпеки ІТ систем та мереж.

Перелік тем для самостійної роботи аспірантів заочної форми навчання

№ з/п	Назва теми
Змістовий модуль 1. Тенденції розвитку і застосування методів і засобів захисту інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів	
1	Тенденції розвитку методів і засобів ведення кібердій і кіберконфліктів
2	Застосування методів і засобів захисту інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів
3	Передумови розвитку методів і засобів ведення кібердій і кіберконфліктів
4	Класифікація форм і способів кібердій
5	Засоби і способи кіберрозвідки
6	Засоби і способи кіберзахисту
Змістовий модуль 2. Проблеми захисту державної інформаційної сфери від стороннього кібернетичного впливу	

№ з/п	Назва теми
7	Проблеми захисту державної інформаційної сфери від стороннього кібернетичного впливу
8	Забезпечення інформаційної безпеки державної інформаційної сфери від стороннього кібернетичного впливу
9	Передумови виникнення загроз для державної інформаційної сфери від стороннього кібернетичного впливу
10	Процеси захисту інформаційно-комунікаційних систем державної інформаційної сфери від стороннього кібернетичного впливу
11	Основні форми і способи стороннього кібернетичного впливу на державну інформаційну сферу
12	Напрями забезпечення кібербезпеки України.
Змістовий модуль 3. Технології та інструменти забезпечення безпеки інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів	
13	Технології забезпечення безпеки інформації в системах і мережах
14	Технологічна модель безпеки інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів
15	Технологічна модель підсистеми інформаційної безпеки
16	Моделі забезпечення безпеки інформації в системах і мережах
17	Стандарт ISO 7498-2 Security Architecture
18	Механізми керування послугами безпеки

Критерії оцінювання самостійної роботи аспіранта

№ 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
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2
3	Дотримання вимог щодо технічного оформлення	1
	Разом	5

6.3. Форми проведення модульного контролю та критерії оцінювання

Оцінка за кожний змістовий модуль включає бали за поточну роботу аспіранта на практичних заняттях, за виконання домашніх завдань, за модульну контрольну роботу. Модульний контроль знань аспіранта здійснюється після завершення вивчення навчального матеріалу модуля. Форма проведення – комп'ютерний тест, що складається з 20 питань закритої та відкритої форм. Модульна контрольна робота оцінюється у 25 балів. Критерії оцінювання модульного контролю наведено у таблиці.

Критерії оцінювання модульного контролю

Сума балів	Значення оцінки
22-25	аспірант виявив повне знання програмного матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу рекомендовану програмою, виявив систематичний характер знань з дисципліни і здатний до самостійного доповнення
13-21	аспірант виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, знайомий з основною рекомендованою літературою
0-13	аспірант, що виявив часткове знання основного програмового матеріалу, не завжди вміє виконувати завдання, передбачені програмою, знайомий лише частково з основною рекомендованою літературою.

6.4 Форми проведення семестрового контролю та критерії оцінювання

Семестровий контроль знань аспірантів здійснюється після завершення вивчення навчального матеріалу дисципліни у формі екзамену. Семестрова рейтингова оцінка аспіранта є сумою підсумкових фактичних оцінок аспіранта за змістовими модулями та балами отриманими за іспит.

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

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

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

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

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

Орієнтовний перелік питань для семестрового контролю

1. Види загроз інформаційній безпеці.
2. Актуальні загрозами національним інтересам та національній безпеці в інформаційній сфері.
3. Технологічна складова інформаційної безпеки держави.
4. Наслідки реалізації загроз національній безпеці в інформаційній сфері.
5. Об’єкти та суб’єкти інформаційної безпеки держави.
6. Принципи забезпечення інформаційної безпеки.
7. Форми і способи забезпечення інформаційної безпеки.
8. Основні методи забезпечення інформаційної безпеки.
9. Технологічна складова інформаційної безпеки держави.
10. Особливості захисту інформації в корпоративних мережах.
11. Групи методи і засоби, що забезпечують безпеку інформації в захищеній обчислювальній мережі.
12. Забезпечення безпеки інформації в призначеній для користувача підсистемі.
13. Захист інформації на рівні підсистеми управління мережею.
14. Захист інформації в каналах зв'язку.
15. Забезпечення контролю достовірності взаємодіючих процесів.
16. Процедура Обмін ідентифікаторами, якщо в мережі використовується симетричне шифрування.
17. Вимоги до системи управління доступом.
18. Вимоги до підсистеми реєстрації і обліку.
19. Вимоги до підсистеми забезпечення цілісності повинна.
20. Основні принципи механізмів захисту від несанкціонованого доступу до інформації.
21. Схеми розташування VPN пристроїв в мережі.
22. Користувальницька схема розташування VPN пристроїв в мережі.
23. Провайдерска схема схема розташування VPN пристроїв в мережі.
24. Використання IPSec для захисту віртуального каналу
25. Протоколи захисту віртуального каналу верхнього рівня архітектура IPSec/
26. Алгоритми аутентифікації для протоколів AH і ESP.
27. Характеристика протоколу заголовка аутентифікації.
28. Характеристика протоколу інкапсулюючого захисту.
29. Базова схема ідентифікації та аутентифікації.
30. Три основних типи профілів доступу пакетна фільтрація.
31. Процес створення профілю доступу ACL.
32. Приклади налаштування профілю доступу ACL.
33. Приклад налаштування комутатора для профілю Ethernet.
34. Приклад налаштування комутатора для профілю IP.
35. Архітектура безпеки корпоративної мережевої інфраструктури.
36. Модель Захмана для корпоративної архітектури.
37. Модель SABSA для корпоративної архітектури.
38. Архітектура та моделі безпеки політики, стандарти, рішення, процедури.

6.5. Оцінювання освітніх досягнень аспірантів за системою ECTS

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

7. Рекомендовані джерела:

Основна:

1. Бурячок В. Л., Хорошко В. О. Технологія прийняття рішень у складних соціотехнічних системах : монографія / В. Л. Бурячок, В. О. Хорошко. – Київ : ДУІКТ, 2012. – 344 с.

2. 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.

3. Бурячок В.Л. Політика інформаційної безпеки: підручник. / В.Л. Бурячок, Р.В.Грищук, В.О.Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 222 с.

4. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. К.: НБУ, 2010.

5. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Звід правил для управління інформаційною безпекою. К.: НБУ, 2010.

Додаткова:

1. Інформаційна безпека держави : навч. посіб. / В. М. Рудницький, С. О. Гнатюк, Н. В. Лада, Р. В. Бреус ; Черкас. держ. технолог. ун-т. – Харків : ДІСА ПЛЮС, 2018. – 359 с.

2. Корченко А. Г. Побудова систем захисту інформації на нечітких множинах/ А. Г. Корченко // Теорія і практичні рішення. – Київ : МК-Пресс, 2016. – 324 с.

3. Endorf C. F. Measuring ROI on security / Carl F. Endorf // Information security management handbook / Edited by H. F. Tipton, M. Krauze. – 6th edition. – Boca Raton : Auerbach Publications, 2017. – Part 1, Section 1.1, Ch. 12. – P. 133–137.

4. Henry K. Risk management and analysis / K. Henry // Information Security Management Handbook / Edited by H. F. Tipton, M. Krauze. – 6th edition. – Boca Raton : Auerbach Publications, 2017. – Part 1, Section 1.4, Ch. 28. – P. 321–329.

5. ISO/IEC 15408-1:2009 «The Common Criteria for Information Technology Security Evaluation. 1: Introduction and general model».

6. ISO/IEC 15408-2:2008 «The Common Criteria for Information Technology Security Evaluation. Security functional components».

7. ISO/IEC 15408-3:2008 «The Common Criteria for Information Technology Security Evaluation. Security assurance components».

8. ISO/IEC Guide 73:2009 «Risk management. Vocabulary. Guidelines for use in standards».

9. Landoll D. The security risk assessment handbook: a complete guide for performing security risk assessments / Douglas J. Landoll. – Boca Raton: Auerbach Publications, 2016. – 504 p.

10. Spedding L., Rose A. Business risk management handbook: a sustainable approach / L. Spedding, A. Rose. – Oxford : Elsevier, 2018. – 768 p.

Додаткові ресурси:

1. Конституція України [Електронний ресурс] : Закон від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / ВР України. – Режим доступу : http://zakon2.rada.gov.ua/laws/(дата звернення: 08.02.2012).

2. Cybercomply: risk-proof your data : Manage all your cyber security and data privacy obligations in one powerful tool [Electronic resource] // Vigilant : web-site. – Access mode: https://www.vigilantsoftware.co.uk/

3. GeNIe Modeler: Complete Modeling Freedom [Electronic resource] // BayesFusion : web-site. – Access mode: https://www.bayesfusion.com/genie/