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
«___» _____ 2022р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРИКЛАДНІ АСПЕКТИ АДМІНІСТРУВАННЯ ТА ЕКСПЛУАТАЦІЇ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

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 математики

Викладач:

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

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

Протокол від 01.09.2022 № 12

Завідувач кафедри _____ (Павло СКЛАДАННИЙ)
(підпис)

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

01.09. 2022

Гарант освітньо-наукової програми _____ (Наталія КОРШУН)
(підпис)

Робочу програму перевірено

01.09. 2022

Завідувач аспірантури, докторантури _____ (Ілона ТРИГУБ)
(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
Вид дисципліни	вибіркова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4/120	
Рік навчання	3	3
Семестр	5	5
Кількість змістових модулів з розподілом:	4	
Обсяг кредитів	4	4
Обсяг годин, в тому числі:	120	120
Аудиторні	32	16
Модульний контроль	8	-
Самостійна робота	80	104
Семестровий контроль	Залік	

2. Мета та завдання навчальної дисципліни

Мета: формування в аспірантів знань, умінь і навичок з застосування теоретичних основ та впровадження технологій забезпечення безпеки ІТ систем та мереж.

Завдання: отримання теоретичних знань та практичних умінь з дослідження теорій і технологій забезпечення безпеки ІТ систем та мереж та набуття наступних компетентностей:

– здатність застосовувати сучасні ІТ технології при створенні систем інформаційної та/або кібербезпеки і захисту інформації;

– здатність робити оцінки та знаходити відповідні рішення щодо застосування систем інформаційної та/або кібербезпеки і захисту інформації;

– здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки ІТ систем та мереж, обробки та перетворення інформації.

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

Програмні компетентності	**Код**	**Значення компетентності**
Фахові компетентності (ФК)	**ФК-3**	Здатність застосовувати сучасні ІТ технології при створенні систем інформаційної та/або кібербезпеки і захисту інформації
	ФК -5	Здатність робити оцінки та в умовах припущень і обмежень знаходити відповідні рішення щодо систем інформаційної та/або кібербезпеки і захисту інформації
	ФК -6	Здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки ІТ систем та мереж, обробки та перетворення інформації

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни аспірант повинен

знати:

– основні алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки;

– принципи побудови та функціонування системи управління інформаційною та/або кібербезпекою організації;

– процеси захисту інформаційно-комунікаційних систем та протоколи коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту;

– порядок впровадження, супроводу та управління комплексними системами захисту інформації в ІКС, проведення їх експертизи та випробувань;

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

вміти:

– 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;

– розробляти та аналізувати проекти ІКС базуючись на стандартизованих технологіях та протоколах передачі даних;

– аналізувати та визначати можливість застосування технологій, методів та засобів КТЗІ в ІКС;

– проектувати та реалізувати комплексні системи КТЗІ в ІКС відповідно до вимог чинних нормативно-правових документів системи захисту інформації;

– 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, впровадження, супроводу та управління комплексними системами захисту інформації в ІКС, проведення їх експертизи та випробувань;

– забезпечувати процеси захисту інформаційно- комунікаційних систем шляхом встановлення та коректної експлуатації програмних га програмно-апаратних комплексів засобів захисту;

– здійснювати захист ресурсів і процесів в ІКС па основі моделей безпеки та встановлених режимів їх безпечного функціонування;

– забезпечувати процеси захисту інформаційно- комунікаційних систем шляхом встановлення та коректної експлуатації програмних та

програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ.

Програмні результати навчання:

Код	Значення програмного результату
ПРз-4	- забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезиекою, 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;
ПРз-5	- розробляти та аналізувати проекти ІКС базуючись на стандартизованих технологіях та протоколах передачі даних; - аналізувати та визначати можливість застосування технологій, методів та засобів КТЗІ в ІКС; - проектувати та реалізувати комплексні системи КТЗІ в ІКС відповідно до вимог чинних нормативно-правових документів системи захисту інформації; - вирішувати задачі, впровадження, супроводу та управління комплексними системами захисту інформації в ІКС, проведення їх експертизи та випробувань; - забезпечувати процеси захисту інформаційно- комунікаційних систем шляхом встановлення та коректної експлуатації програмних га програмно-апаратних комплексів засобів захисту;
ПРз-6	- розробляти та впроваджувати дослідницькі проекти в сфері захисту інформації, інформаційної та кібербезпеки; - розробляти алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки; - здійснювати захист ресурсів і процесів в ІКС па основі моделей безпеки та встановлених режимів їх безпечного функціонування; - забезпечувати процеси захисту інформаційно- комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ; - забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками з врахуванням можливих конфліктів і катастроф;

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назви змістових модулів і тем	Усього	Розподіл годин між видами робіт			
		Аудиторна			Самостійна
		Лекції	Практичні	Семінарські	
Змістовий модуль І. Основи проектування та технологія розроблення системи захисту ІТ систем та мереж від стороннього кібервпливу					
Тема 1. Основи проектування та технологія розроблення системи захисту ІТ систем та мереж від стороннього кібервпливу	28	4	2	2	20
Модульний контроль	2				
Разом	**30**	**4**	**2**	**2**	**20**
Змістовий модуль ІІ. Сучасні методи і засоби аналізу та оцінки систем інформаційної та/або кібербезпеки і захисту інформаці					
Тема 2. Сучасні методи і засоби аналізу та оцінки систем інформаційної та/або кібербезпеки і захисту інформаці	28	4	2	2	20
Модульний контроль	2				
Разом	**30**	**4**	**2**	**2**	**20**
Змістовий модуль ІІІ. Технології та інструменти забезпечення безпеки інформації в системах і мережах.					
Тема 3. Технології та інструменти забезпечення безпеки інформації в системах і мережах.	28	4	2	2	20
Модульний контроль	2				
Разом	**30**	**4**	**2**	**2**	**20**
Змістовий модуль ІV. Технології адміністрування та експлуатації захищених ІТ систем і мереж					
Тема 4. Технології адміністрування та експлуатації захищених ІТ систем і мереж	28	4	2	2	20
Модульний контроль 4	2				
Разом	**30**	**4**	**2**	**2**	**20**
Усього	**120**	**16**	**8**	**8**	**80**

Тематичний план для заочної форми навчання

Назви змістових модулів і тем	Усього	Розподіл годин між видами робіт			
		Аудиторна			Самостійна
		Лекції	Практичні	Лабораторні	
Змістовий модуль І. Основи проектування та технологія розроблення системи захисту ІТ систем та мереж від стороннього кібервпливу					
Тема 1. Основи проектування та технологія розроблення системи захисту ІТ систем та мереж від стороннього кібервпливу	30	2	2		26
Разом	**30**	**2**	**2**		**26**
Змістовий модуль ІІ. Сучасні методи і засоби аналізу та оцінки систем інформаційної та/або кібербезпеки і захисту інформації					
Тема 2. Сучасні методи і засоби аналізу та оцінки систем інформаційної та/або кібербезпеки і захисту інформаці	30	2		2	26
Разом	**30**	**2**		**2**	**26**
Змістовий модуль ІІІ. Технології та інструменти забезпечення безпеки інформації в системах і мережах.					
Тема 3. Технології та інструменти забезпечення безпеки інформації в системах і мережах.	30	2	2		26
Разом за змістовим модулем	**30**	**2**	**2**		**26**
Змістовий модуль ІV. Технології адміністрування та експлуатації захищених ІТ систем і мереж					
Тема 4. Технології адміністрування та експлуатації захищених ІТ систем і мереж	30	2		2	26
Разом	**30**	**2**		**2**	**26**
Усього	**120**	**8**	**4**	**4**	**104**

5. Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ І. Основи проектування та технологія розроблення системи захисту ІТ систем та мереж від стороннього кібервпливу

Тема 1. Основи проектування та технологія розроблення системи захисту ІТ систем та мереж від стороннього кібервпливу

Принципи побудови та вихідні дані для проектування систем захисту ІТ систем. Особливості реалізації атак на захищені ІТ системи та основні уразливості таких систем, ризики функціонування захищених ІТ систем в умовах стороннього кібервпливу.

Постановка завдання на проектування системи захисту та особливості його реалізації. Методологія та методи проектування систем захисту ІТ систем. Засоби проектування та їх класифікація . Методології моделювання предметної області. Функціонально- та об'єктно-орієнтовані методології структурного моделювання. Основні методології проектування систем захисту ІТ систем.

Ключові слова: захищені ІТ системи, методологія та методи проектування систем захисту, проектування захищених інформаційних систем.

Література:

1. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2015. – 449 с.

2. Литвинов В.В., Голуб С.В. Об'єктно-орієнтоване моделювання при проектуванні вбудованих систем і систем реального часу. – Черкаси: ЧНУ ім. Богдана Хмельницького, 2011. – 376 с.

3. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT)

4. Богуш В.М., Довидьков О.А., Кривуца В.Г. Основи захищених інформаційних технологій. – К.: ДУІКТ, 2010. – 454 с.

ЗМІСТОВИЙ МОДУЛЬ ІІ. Сучасні методи і засоби аналізу та оцінки систем інформаційної та/або кібербезпеки і захисту інформаці

Тема 2. Сучасні методи і засоби аналізу та оцінки систем інформаційної та/або кібербезпеки і захисту інформаці

Методологія аналізу захищеності інформаційної системи. Стандартизація підходів до забезпечення інформаційної безпеки. Забезпечення інтегральної безпеки інформаційних систем і мереж.

Алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки. Процеси захисту інформаційно-комунікаційних систем.

Ключові слова: аналіз захищеності, технологічна модель, технологічна модель інформаційної безпеки, концепція захищених мереж, забезпечення інформаційної безпеки, інструменти забезпечення безпеки інформації.

Література:

1. 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.

2. 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.

3. Бурячок В.Л. Технологія прийняття рішень у складних соціотехнічних системах: монографія. / В.Л. Бурячок, В.О.Хорошко. / Під заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ДУІКТ, 2012. – 344 с.

4. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT) http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797

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

6. 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.

ЗМІСТОВИЙ МОДУЛЬ ІІІ. Технології та інструменти забезпечення безпеки інформації в системах і мережах

Тема 3. Технології та інструменти забезпечення безпеки інформації в системах і мережах

Технологічна модель підсистеми інформаційної безпеки. Технології нижнього рівня захисту інформації в системах інформаційної та/або кібербезпеки. Концепція захищених віртуальних приватних мереж.

Протоколи коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту.

Ключові слова: технологічна модель, алгоритми, моделі, методи, програмні комплекси кібербезпеки.

Література:

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. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT) http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797

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

6. 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.

ЗМІСТОВИЙ МОДУЛЬ ІV. Технології адміністрування та експлуатації захищених ІТ систем і мереж

Тема 4. Технології адміністрування та експлуатації захищених ІТ систем і мереж

Адміністрування процесів введення в експлуатацію та експлуатації захищених ІТ систем і мереж. Перевірка і підтримка цілісності даних. Розмежування прав доступу та правила забезпечення безпеки даних.

Удосконалення, модернізація та уніфікація систем, засобів і технологій забезпечення безпеки ІТ систем та мереж, обробки та перетворення

інформації.

Ключові слова: 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.

Література:

1. 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.

2. 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.

3. Бурячок В.Л. Технологія прийняття рішень у складних соціотехнічних системах: монографія. / В.Л. Бурячок, В.О.Хорошко. / Під заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ДУІКТ, 2012. – 344 с.

4. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT) http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797

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

6. 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.

6. Контроль навчальних досягнень

6.1. Система оцінювання навчальних досягнень аспірантів денної форми навчання

№ з/п	Вид діяльності аспіранта	Макс. кільк. балів заодиницю	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
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	**100/348=0,29**								

Система оцінювання навчальних досягнень аспірантів заочної форми навчання

№ з/п	Вид діяльності аспіранта	Макс. кільк. балів заодиницю	Модуль 1		Модуль 2		Модуль 3		Модуль 4	
			Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів	Кільк.од	Кільк.один.	Макс. кільк. балів	Кільк.один.
1	Відвідування лекцій	1	1	1	1	1	1	1	1	1
2	Відвідування практичних занять	1	1	1	1	1	1	1	1	1
3	Відвідування семінарських занять									
4	Робота на практичних заняттях	10	1	10	1	10	1	10	1	10
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**		**42**
7	Максимальна кількість балів:	**103**								
9	Розрахунок коефіцієнта Бал max / Сума балів max	**100/168=0,6**								

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 першоджерела за запропонованою тематикою. Огляд представити у вигляді наукового реферату за вибраною темою з прикладами з предметної області.

Завдання для самостійної роботи аспірантів денної форми навчання

№ з/п	Назва теми
Змістовий модуль 1. Основи проектування та технологія розроблення системи захисту ІТ систем та мереж від стороннього кібервпливу	
1	Принципи побудови та вихідні дані для проектування систем захисту ІТ систем
2	Методологія та методи проектування систем захисту ІТ систем
3	Основні методології проектування систем захисту ІТ систем
Змістовий модуль 2. Сучасні методи і засоби аналізу та оцінки систем інформаційної та/або кібербезпеки і захисту інформаці	
4	Методологія аналізу захищеності інформаційної системи
5	Стандартизація підходів до забезпечення інформаційної безпеки
6	Алгоритми, моделі, методи оцінки характеристик і стану систем інформаційної та кібербезпеки.
Змістовий модуль 3. Технології та інструменти забезпечення безпеки інформації в системах і мережах	
7	Технології забезпечення безпеки інформації в системах і мережах
8	Технологічна модель підсистеми інформаційної безпеки
9	Протоколи коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту
Змістовий модуль 4. Технології адміністрування та експлуатації захищених ІТ систем і мереж	
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.

Завдання для самостійної роботи аспірантів заочної форми навчання

№ з/п	Назва теми
Змістовий модуль 1. Основи проектування та технологія розроблення системи захисту ІТ систем та мереж від стороннього кібервпливу	
1	Принципи побудови та вихідні дані для проектування систем захисту ІТ систем
2	Ризики функціонування захищених ІТ систем в умовах стороннього кібервпливу

3	Методологія та методи проектування систем захисту ІТ систем
4	Засоби проектування та їх класифікація. Методології моделювання предметної області
5	Основні методології проектування систем захисту ІТ систем
6	Функціонально- та об'єктно-орієнтовані методології структурного моделювання систем захисту
Змістовий модуль 2. Сучасні методи і засоби аналізу та оцінки систем інформаційної та/або кібербезпеки і захисту інформаці	
7	Методологія аналізу захищеності інформаційної системи
8	Стандартизація підходів до забезпечення інформаційної безпеки
9	Забезпечення інтегральної безпеки інформаційних систем і мереж
10	Алгоритми, моделі, методи оцінки характеристик і стану систем інформаційної та кібербезпеки.
11	Складні програмні комплекси оцінки стану систем інформаційної та кібербезпеки
12	Процеси захисту інформаційно-комунікаційних систем.
Змістовий модуль 3. Технології та інструменти забезпечення безпеки інформації в системах і мережах	
13	Технології забезпечення безпеки інформації в системах і мережах
14	Інструменти забезпечення безпеки інформації в системах і мережах
15	Технологічна модель підсистеми інформаційної безпеки
16	Технології нижнього рівня захисту інформації в системах інформаційної безпеки
17	Концепція захищених віртуальних приватних мереж
18	Протоколи коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту
Змістовий модуль 4. Технології адміністрування та експлуатації захищених ІТ систем і мереж	
19	Адміністрування процесів введення в експлуатацію захищених ІТ систем і мереж
20	Адміністрування процесів експлуатації захищених ІТ систем і мереж
21	Перевірка і підтримка цілісності даних
22	Розмежування прав доступу та правила забезпечення безпеки даних
23	Удосконалення систем, засобів і технологій забезпечення безпеки ІТ систем та мереж.
24	Модернізація та уніфікація систем, засобів і технологій забезпечення безпеки ІТ систем та мереж.

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,	2

	визначення перспектив дослідження	
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 заліку. Підсумкова семестрова (залікова) рейтингова оцінка аспіранта є сумою підсумкових фактичних оцінок аспіранта за змістовими модулями.

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 – досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Рекомендовані джерела:

Основні (базові):

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. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT) http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797
5. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. К.: НБУ, 2010.
6. 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.

Додаткові:

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. Построение систем защиты информации на нечетких множествах / А. Г. Корченко // Теория и практические решения. – 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. Gilmore Robert. Catastrophe Theory of Scientists and Engineers. New York: Dover, 1993.

5. 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.

6. ISO/IEC 13335:2000 «Information technology. Guidelines for the management of IT Security. Part 4: Selection of safeguards».

7. ISO/IEC 13335-1:2004 «Information technology. Security techniques. Management of information and communications technology security».

8. ISO/IEC 13335-3:1998 «Information technology. Guidelines for the management of IT Security. Part 3: Techniques for the management of IT Security».

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

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

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

12. ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements».

13. ISO/IEC 27002:2005 «Information technology. Security techniques. Code of practice for information security management».

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

15. ISO/IEC TR 18044:2004 «Information technology. Security techniques. Information security incident management».

16. ISO/TR 13569:2005 «Financial services - Information security guidelines».

17. 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.

18. Sanns, Werner. Catastrophe Theory with Mathematica: A Geometric Approach. Germany: DAV, 2000

19. 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/