Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та управління

Кафедра інформаційної та кібернетичної безпеки

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ О.Б. Жильцов
«31» 01 2019 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ»

для студентів

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

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 2068/19
(підпис) (прізвище, ініціали)
«___» _____ 20 19 р.

Київ-2019

Розробник:

Семко Віктор Володимирович, доктор технічних наук, доцент, професор кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Викладачі:

Семко Віктор Володимирович, доктор технічних наук, доцент, професор кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки

Протокол від 16.01.2019 р. № 1

Завідувач кафедри _____ В.Л. Бурячок
(підпис)

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

___.___. 20___ р.

Керівник освітньої програми _____ В.В. Семко
(підпис)

Робочу програму перевірено

___.___. 20___ р.

Заступник директора/декана _____ І.Ю. Мельник
(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)

Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	2 / 60	
Курс	1	
Семестр	2	
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 «Теоретичні аспекти захищених інформаційно-комунікаційних технологій» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека, освітньої 125.00.01 «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 «Теоретичні аспекти захищених інформаційно-комунікаційних технологій» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Теоретичні аспекти захищених інформаційно-комунікаційних технологій» складається з 2-х змістових модулів: 1. Основні парадигми і моделі захисту інформації від несанкціонованого доступу в обчислювальних системах. 2. Політика безпеки,стандартизовані моделі, принципи побудови і напрямки розвитку сучасних технологій створення захищених інформаційно-комунікаційних систем. Обсяг дисципліни – 60 год. (2 кредити).

Метою викладання навчальної дисципліни «Теоретичні аспекти захищених інформаційно-комунікаційних технологій» є отримання компетентностей та навичок щодо обґрунтування застосування механізмів захисту та оцінки рівня захищеності інформаційно-комунікаційних систем і технологій від несанкціонованого доступу до ресурсів.

Завдання:

- надання студентам теоретичних знань щодо проблем, завдань і особливостей технологій захисту інформації на об'єктах інформаційної діяльності від несанкціонованого доступу до ресурсів;

– формування у студентів категоріальних понять з основ процесів, що притаманні функціонуванню об’єктів інформаційної діяльності в умовах зовнішніх і внутрішніх негативних впливів;

– формування у студентів знань і умінь щодо формування політики безпеки інформаційно-комунікаційних систем;

– стимулювання студентів до активної аналітико-пошукової роботи, що спрямована на визначення ефективних шляхів розвитку у сфері захисту інформації.

У результаті вивчення навчальної дисципліни формуються

загальні компетентності:

КЗ-2: Здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях

КЗ-3: Здатність до виявлення, генерування, дослідження та вирішення проблем за професійним спрямуванням.

фахові компетентності:

КФ-1: Здатність до застосування сучасних інформаційних і безпекових технологій у сфері захисту інформації

КФ-5: Здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації.

. Результати навчання за дисципліною

При вивченні курсу «Теоретичні аспекти захищених інформаційно-комунікаційних технологій» студенти повинні

знати:

- про правові і нормативні акти, які визначають систему захисту інформації від несанкціонованого доступу;
- про сутність сучасної теорії захищених інформаційних систем;
- про сукупність основних теоретичних положень складових захищених інформаційних технологій: гарантовано захищених обчислювальних систем; процесів забезпечення безпеки обчислювальних систем; механізмів захисту інформаційних технологій; програмного забезпечення для вирішення завдань захисту інформації; критеріїв безпеки інформаційних технологій;
- про основні моделі, методи, принципи і правила побудови систем захисту інформації від несанкціонованого доступу на об’єктах інформаційної діяльності (інформаційно-комунікаційних системах);
- особливості забезпечення безпеки сучасних інформаційних технологій.

уміти:

- обґрунтовувати застосування механізмів захисту та оцінки рівня захищеності інформаційної системи (технології);
- визначати моделі, принципи і правила побудови систем захисту від несанкціонованого доступу об’єктів і інформаційно-комунікаційних систем;
- моделювати основні процеси забезпечення безпеки об’єктів і інформаційно-комунікаційних систем.

та досягнути наступні ***програмні результати***:

ПРз-2: - вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки;

- вміти оцінювати уразливості й методи їх застосування в різних інформаційно-комунікаційних технологіях;

- вміти обґрунтовувати основні вимоги до програмного забезпечення, що вирішує завдання захисту інформації;

- вміти обґрунтовувати застосування національних та міжнародних стандартів безпеки інформаційних технологій;
- вміти характеризувати особливості забезпечення безпеки сучасних інформаційних технологій;

ПРз-3: - знати методи оцінки вразливостей й методи оцінки ефективності систем захисту інформації від несанкціонованого доступу інформаційно-комунікаційних системах;
- вміти виявляти ризики експлуатації загроз несанкціонованого доступу до ресурсів інформаційно-комунікаційних систем
- вміти обґрунтовувати положення політики захисту інформації від несанкціонованого доступу в інформаційно-комунікаційних системах;

ПРз-7: - вміти оцінювати загрози інформації в інформаційно-комунікаційних системах;
- вміти визначати вимоги до методів і способів попередження експлуатації загроз несанкціонованого доступу до ресурсів інформаційно-комунікаційних систем;

ПРз-9: - володіти практичними навичками формування вимог до політики безпеки інформаційно-комунікаційних систем.

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. Основні парадигми і моделі захисту інформації від несанкціонованого доступу в обчислювальних системах							
Тема 1. Основні поняття розроблення гарантовано захищених інформаційних технологій.	6	2					4
Тема 2. Загальні моделі опису функціонування комп'ютерних систем.	12	2		2	2		6
Тема 3. Основи теорії захищених систем.	10	2		2	2		4
Модульний контроль	2						
Разом	30	6		4	4		14
Змістовий модуль 2. Політика безпеки,стандартизовані моделі, принципи побудови і напрямки розвитку сучасних технологій створення захищених інформаційно-комунікаційних систем							
Тема 4. Забезпечення гарантій виконання вимог політик безпеки.	6	2					4
Тема 5. Стандартизовані моделі опису сучасних інформаційних технологій та методи оцінки їх ефективності.	12	2		2	2		6
Тема 6. Приклади побудови сучасних захищених інформаційних технологій.	10	2		2	2		4
Модульний контроль	2						
Разом	30	6		4	4		14
Усього	60	12		8	8		28

5. Програма навчальної дисципліни

Змістовий модуль 1. Основні парадигми і моделі захисту інформації від несанкціонованого доступу в обчислювальних системах

Тема 1. Вступ. Основні поняття розроблення гарантовано захищених інформаційних технологій

Основні поняття гарантовано захищених інформаційних технологій: етапи розвитку парадигм захисту інформації; основні поняття теорії захисту інформації та їх взаємозв'язок; помилки під час розроблення систем захисту як причина появи уразливостей автоматизованих систем; типи каналів порушення безпеки критичної інформації; поняття про гарантовано захищені інформаційні технології; основні принципи розроблення систем захисту інформації.

Основи формування гарантовано захищених інформаційних технологій: використання концепції ієрархічної декомпозиції для побудови систем захисту; поняття про доказовий підхід до побудови систем захисту; приклад використання доказового підходу; взаємозв'язок доказового та нормативного підходів; використання доказового підходу на прикладі національних критеріїв оцінки захищеності; поняття про довірчу обчислювальну базу; поняття про концепцію диспетчера доступу.

Основи розроблення гарантованих систем захисту: система методів забезпечення заданого рівня гарантій захисту. Система нормативних документів із забезпечення захисту інформації в комп'ютерних системах та мережах. Перспективні напрямки розвитку методів створення систем захисту.

Тема 2. Загальні моделі опису функціонування комп'ютерних систем

Моделі опису функціонування комп'ютерних систем: суб'єктно-об'єктна модель опису комп'ютерної системи; автоматна суб'єктно-об'єктна модель опису комп'ютерної системи; використання суб'єктно-об'єктної моделі для опису базових операції в комп'ютерній системі.

Підходи до формування моделі загроз. Підходи до формування моделі порушника.

Підходи та моделі опису цінності інформації: базові поняття; адитивна модель цінності інформації; порядкова шкала цінностей; модель решітки цінностей; MLS решітка.

Підходи та моделі оцінки збитків автоматизованої системи та ризику її функціонування.

Тема 3. Основи теорії захищених систем

Політики управління доступом: визначення поняття політика безпеки; поняття про гранулювання захисту; мандатна політика безпеки; дискреційна політика безпеки; ролева політика безпеки; довірча та адміністративна політики безпеки.

Моделі опису політики безпеки: класифікація моделей безпеки за типами загроз; класифікація моделей безпеки за підходами до захисту.

Моделі забезпечення конфіденційності: моделі дискреційного доступу; моделі забезпечення конфіденційності; спеціалізовані моделі безпеки; Інформаційні моделі (моделі інформаційних потоків); імовірнісні моделі.

Моделі забезпечення цілісності: модель Байба; моделі із змінними рівнями суб'єктів та об'єктів; модель Кларка-Вільсона; модель контролю цілісності ядра системи.

Моделі забезпечення доступності: основні поняття щодо забезпечення доступності; мандатна модель забезпечення доступності; модель Міллена розподілення ресурсів.

Приклади моделювання питань безпеки в обчислювальних системах: моделі захисту централізованих та розподілених операційних систем; моделі захисту деяких типових технологій оброблення інформації; моделі безпеки середовищ розроблення та функціонування прикладного програмного забезпечення.

Основи синтезу моделей безпеки: методика синтезу моделей безпеки; приклад синтезу гарантовано захищеної автоматизованої системи; приклад використання результатів синтезу моделей безпеки для доведення гарантованості захисту систем.

Змістовий модуль 2. Політика безпеки,стандартизовані моделі, принципи побудови і напрямки розвитку сучасних технологій створення захищених інформаційно-комунікаційних систем

Тема 4. Забезпечення гарантій виконання вимог політик безпеки

Загальні поняття про розроблення програмного забезпечення захисту інформації: особливості розроблення програмного забезпечення захисту інформації; надійність та стійкість програмного забезпечення; методи забезпечення надійності програмного забезпечення.

Технологічна безпека розроблення систем захисту: технологічна березка програмного забезпечення; формування інструментально-технологічних комплексів; формування моделюючих комплексів.

Забезпечення гарантій виконання політики безпеки на основі методу генерації ізольованих програмних середовищ: співвідношення гарантій виконання політики безпеки з поняттям ізольованого програмного середовища; методо генерації ізольованого програмного середовища при проектуванні механізмів гарантованої підтримки політики безпеки; реалізація гарантій виконання заданої політики безпеки.

Тема 5. Стандартизовані моделі опису сучасних інформаційних технологій та методи оцінки їх ефективності

Модель, що покладена в основу міжнародного стандарту ISO 7498-2: ієрархічна декомпозиція в моделі ISO/OSI; загрози в архітектурі відкритих мереж; процедури захисту; сервісні служби захисту; реалізація захисту; адміністрування засобів безпеки.

Модель, що покладена в основу НД ТЗІ 2.5: загальні положення моделі; функціональні критерії НД ТЗІ 2.5; критерії гарантій безпеки НД ТЗІ 2.5; функціональні профілі захищеності інформації НД ТЗІ 2.5.

Модель, що покладена в основу міжнародного стандарту ISO 15408: основні положення загальних критеріїв безпеки інформаційних технологій; потенційні загрози безпеці та типові завдання захисту; політика безпеки; продукт інформаційних технологій; профіль захисту; проект захисту; функціональні вимоги до засобів захисту; вимоги гарантій засобів захисту; рівні гарантій безпеки; шляхи та перспективи застосування загальних критеріїв в Україні.

Тема 6. Приклади побудови сучасних захищених інформаційних технологій

Розвиток захищених обчислювальних систем.

Огляд деяких захищених обчислювальних систем.

Сучасні захищені середовища та їх моделі: типові умови функціонування розподілених обчислювальних середовищ з точки зору забезпечення їх цілісності; типові захищені розподілені обчислювальні середовища.

Багаторівневі системи на основі реляційних систем управління базами даних: приклад предметної частини; декомпозиція баз даних; декомпозиція на рівні відносин.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної 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	3	3	3	3
Відвідування семінарських занять	1				
Відвідування практичних занять	1	2	2	2	2
Відвідування лабораторних занять	1	2	2	2	2
Робота на семінарському занятті	10				
Робота на практичному занятті	10	2	20	2	20
Лабораторна робота (в тому числі допуск, виконання, захист)	10	2	20	2	20
Виконання завдань для самостійної роботи	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25
Виконання ІНДЗ	30				
	Разом	-	77	-	77
	Максимальна кількість балів: 154				
	Розрахунок коефіцієнта: 154/100=1,54				

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. Основні парадигми і моделі захисту інформації від		14	5

несанкціонованого доступу в обчислювальних системах			
1	Тема 1. Основні поняття розроблення гарантовано захищених інформаційних технологій. Тема 2. Загальні моделі опису функціонування комп'ютерних систем. Тема 3. Основи теорії захищених систем.	14	5
Змістовий модуль 2. Політика безпеки,стандартизовані моделі, принципи побудови і напрямки розвитку сучасних технологій створення захищених інформаційно-комунікаційних систем		14	5
2	Тема 4. Забезпечення гарантій виконання вимог політик безпеки. Тема 5. Стандартизовані моделі опису сучасних інформаційних технологій та методи оцінки їх ефективності. Тема 6. Приклади побудови сучасних захищених інформаційних технологій.	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 – комп'ютерний тест, що складається 20 запитань закритої та відкритої форм.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

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

Орієнтовний перелік питань для самоконтролю

1. Визначити поняття нелегітимного доступу як каналу потенційного порушення безпеки в системі. Наведіть приклади.
2. Визначити поняття комп'ютерна система. Дослідити фізичну і логічну сутність комп'ютерної системи.
3. Визначеити поняття абсолютно захищеній інформаційній технології. Навести приклади.
4. Визначити поняття рівня гарантій безпеки комп'ютерної системи, Наведіть приклад вимог до гарантій захищеності в політиці безпеки обчислювальної системи.
5. Визначити і дослідити основні принципи розроблення і впровадження засобів захисту інформації в обчислювальних системах.
6. Визначити сутність принципу системності, як одного з основних принципів розроблення

засобів захисту інформації в обчислювальних системах.

7. Визначити сутність конфепції ієрархічної декомпозиції при побудові систем захисту інформації. Дослідити систему формальних мов опису поведінки обчислювальної системи на рівнях її функціонування.
8. Визначити поняття політики безпеки інформації в обчислювальній системі. Навести прикліди політики безпеки інформації в обчислювальній системі.
9. Визначити принцип описового підходу в теорії інформаційної безпеки. Навести приклади.
10. Визначити поняття рівня захищеності обчислювальної системи. Навести приклади формальної оцінки рівня захищеності.
11. Дослідити властивості захищених обчислювальних систем. Навести приклади.
12. Визначити поняття гарантії проведення політики безпеки інформації, як міри довіри до архітектурних і технологічних рішень при побудові обчислювальної системи.
13. Визначити сутність понять суб'єктів і об'єктів обчислювальної системи Навести приклади.
14. Визначити сутність поняття порядкової шкали цінностей. Навести приклади.
15. Визначити і дослідити особливості праксеологічного підходу до створення і функціонування систем захисту інформації.
16. Визначити і дослідити сутність моделі порушника при розробці політики безпеки об'єктів інформаційної діяльності. Навести приклади.
17. Визначити і дослідити сутність методів і моделей аналізу ризиків при створенні систем захисту інформації на об'єктах інформаційної діяльності.
18. Визначити і дослідити сутність квазіекономічного підходу до оцінки інформації в обчислювальних системах. Навести приклади.
19. Визначити і дослідити сутність методів оцінки цінності інформації. Навести приклади
20. Визначити і дослідити набір норм, правил і практичних прийомів, що регламентують управління, захист і розподіл цінної інформації в політиці безпеки об'єктів інформаційної діяльності.
21. Визначити і дослідити сутність мандатної політики безпеки інформації. Навести приклади.
22. Визначити і дослідити сутність дискреційної політики безпеки інформації. Навести приклади.
23. Визначити і дослідити сутність і відмінність довірчої та адміністративної моделей доступу в обчислювальних системах. Навести приклади.
24. Навести класифікацію моделей безпеки за типами загроз, визначити і дослідити їх сутність. Навести приклади.
25. Визначити і дослідити сутність моделі Харрісона-Руссо-Ульмана. Навести приклади.
26. Дослідити сутність сновної теореми безпеки Белла-ЛаПадули. Навести приклади.
27. Визначити і дослідити сутність ланкової моделі забезпечення конфіденційності інформації в обчислювальних системах. Навести приклади.
28. Визначити і дослідити сутність моделі Байба. Навести приклади.
29. Визначити і дослідити сутність формального (математичного) опису правил NRD. Навести приклади.
30. Визначити і дослідити сутність моделі Кларка-Вільсона. Навести приклади.
31. Визначити і дослідити сутність кілець моделі контролю цілісності ядра обчислювальної системи. Навести приклади.

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 – 12 год., практичні заняття –8 год., лабораторні роботи – 8 год., модульний контроль –4 год., самостійна робота –28 год.

Модулі (назви, бали)	**Змістовий модуль 1. Методи виявлення та оцінки загроз інформації (77 балів)**				**Змістовий модуль 2. Визначення вихідних даних щодо створення КСЗІ в ІТС (77 балів)**	
Лекції (теми, бали)	Методи та види несанкціонованого доступу та канали витоку інформації (1 бал)	Поняття дестабілізуючих факторів та моделі реалізації загроз інформації (1 бал)		Структура критеріїв захищеності інформації та послуг, що забезпечують захист від загроз (1 бал)	Порядок обстеження середовищ функціонування ІТС (1 бал)	Методи оцінки загроз інформації (2 бали)
Практичні, семінарські заняття (теми, бали)	Нормативно-правові акти у сфері захисту інформації (11 балів)	Основні нормативно-правові акти, що регламентують питання захисту інформації в ІКС. (11 балів)			Порядок обстеження середовищ функціонування ІТС (11 балів)	Формування вихідних даних щодо створення КСЗІ в ІТС (11 балів)
Лабораторні заняття (теми, бали)		Нормативно-правові акти у сфері захисту інформації (11 балів)		Основні нормативно-правові акти, що регламентують питання захисту інформації в ІКС. (11 балів)	Обстеження середовищ функціонування ІТС підприємства (11 балів)	Формування вихідних даних щодо створення КСЗІ в ІТС (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

1. Богуш В.М. і Довидьков О.А. Основи захищених інформаційних технологій. – К.: ДУІКТ, 2005 - 450 с.
2. Бурячок В.Л., Семко В.В., Складанний П.М. і Лукова-Чуйко Н.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. – К.: ДУТ - КНУ, 2016. – 178с.

Додаткова

3. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: термінологічний навчальний довідник. – К.: ООО “Д.В.К.” 2004. – 508 с.
4. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации.– М.: Изд-во агентства "Яхтсмен", 1996.– 192 с.
5. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия-Телеком,2000. – 452 с.
6. Иванова Г.С. Технология программирования: Учебник для вузов. — М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. — 320 с.
7. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
8. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
9. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
10. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
11. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розроблення технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
12. Теоретические основы компьютерной безопасности: Учебное пособие для вузов / П.Н.Девянин, О.О.Михальский, Д.И.Правиков и др. – М.: Радио и связь, 2000. – 192 с.
13. Common Criteria for Information Technology Security Evaluation. National Institute of Standards and Technology \& National Security Agency (USA), Communication Security Establishment (Canada), UK IT Security and Certification Scheme (United Kingdom), Bundesamt fur Sichereit in der Informationstechnik (Germany), Service Central de la Securite des Systemes (France), National Communications Security Agency (Netherlands). Version 2.1. August 1999.
14. Common Methodology for Information Technology Security Evaluation. National Institute of Standards and Technology \& National Security Agency (USA), Communication Security Establishment (Canada), UK IT Security and Certification Scheme (United Kingdom), Bundesamt fur Sichereit in der Informationstechnik (Germany), Service Central de la Securite des Systemes (France), National Communications Security Agency (Netherlands). Version 0.95. June 2000.
15. ISO/IEC 7498-2. Information processing systems Open Systems Interconnection Basic Reference Model. Part 2: Security Architecture. Switzeland, 1989. 32 pp.

9. Додаткові ресурси

1. Руководства пользователя коммутаторов D-Link и учебные материалы компании D-Link [электронный ресурс] ftp://ftp.dlink.ru/
2. Бараш Л. Коммутаторы в локальных сетях. [электронный ресурс] http://desna.kiev.ua
3. History of LAN Switching. [электронный ресурс] http://www.myipaddressinfo.com

4. Evolution: 20 years of switching fabric. Ori Aruj, Dune Networks [электронный ресурс] http://www.commsdesign.com

5. On-chip Global Interconnects for Networking ASICs [электронный ресурс] http://www.lsi.com

6. Andreas D. Bovopoulos and Micha Zeiger. Shared-Memory Fabrics Meet 10-Gbit Backplane Demands. TeraChip, Inc. [электронный ресурс] http://www.commsdesign.com

7. Matching Output Queueing with a Combined Input Output Queued Switch [электронный ресурс] http://www-rcf.usc.edu

8. An improved algorithm for CIOQ switches. Yossi Azar, Ybssi Richter. [электронный ресурс] http://portal.acm.org

9. Сайт научной базы данных «SciVerse ScienceDirect» [электронный ре-сурс] http://www.sciencedirect.com

10. Сайт Института инженеров по электротехнике и электронике (IEEE, Institute of Electrical and Electronics Engineers) [электронный ресурс] http://www.ieee.org