Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та математики

Кафедра інформаційної та кібернетичної безпеки

імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«___»_____ 2023

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ПРОГРАМНІ КОМПЛЕКСИ ЗАХИСТУ АС ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ»

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
Протокол № 2971/23
(підпис) (прізвище, ініціали)
«___» 2023 р.

2023 – 2024 навчальний рік

Розробник:
Козачок Валерій Анатолійович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:
Козачок Валерій Анатолійович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Протокол від 01.09.2022 р. № 12

Завідувач кафедри _____ (підпис) Павло СКЛАДАННИЙ

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

___.___. 2022 р.
Керівник освітньої програми _____ (підпис) Артем ПЛАТОНЕНКО

Робочу програму перевірено
___.___. 2022 р.
Заступник декана _____ (підпис) Євген ІВАНІЧЕНКО

Пролонговано:
на 2023/2024 н.р. _____ (підпис) (Складанний П.І.), «23» 08 2023 р., протокол № 8
на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___
на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___
на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 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	5 / 150	
Курс	3	
Семестр	6	
Кількість змістових модулів з розподілом:	1	
Обсяг кредитів	5	
Обсяг годин, в тому числі:	150	
Аудиторні	56	
Модульний контроль	8	
Семестровий контроль	30	
Самостійна робота	56	
Форма семестрового контролю	екзамен	

1. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Програмні комплекси захисту АС від несанкціонованого доступу» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека та захист інформації галузі знань 12 «Інформаційні технології».

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач другого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Програмні комплекси захисту АС від несанкціонованого доступу» та необхідне методичне забезпечення, складові і технологію

Навчальна дисципліна «Програмні комплекси захисту АС від несанкціонованого доступу» складається з одного змістового модулю: Програмні комплекси захисту АС від несанкціонованого доступу. Обсяг дисципліни – 150 год. (5 кредитів).

Метою викладання навчальної дисципліни «Програмні комплекси захисту АС від несанкціонованого доступу» є:

- вивчення основних підходів до забезпечення інформаційної безпеки в організаціях різної форми власності;
- ґрунтовне ознайомлення студентів із основними програмними комплексами захисту АС від несанкціонованого доступу в галузі інформаційної безпеки та особливостями їх застосування на практиці;
- ознайомлення студентів із основними типами технологічних рішень направленими на забезпечення інформаційної безпеки;
- формування у студентів знань, вмінь і навичок щодо впровадження та застосування теоретичних знань щодо забезпечення інформаційної безпеки в майбутній професійної діяльності.

Завдання полягає у:

- наданні студентам базових теоретичних і практичних знань в використанні програмних комплексів захисту АС від несанкціонованого доступу у галузі інформаційної безпеки;
- наданні студентам базових знань щодо процесу створення безпечних інформаційних систем та процесів підтвердження їх відповідності;
- набутті студентами практичних навичок застосування сучасних технологій забезпечення інформаційної безпеки;
- вивченні основних принципів забезпечення інформаційної безпеки.

Фахові компетентності навчальної дисципліни:

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.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен

знати:

- основні вітчизняні нормативні документи в галузі захисту інформації та міжнародні стандарти з інформаційної безпеки, процеси які формалізуються ними при управлінні програмними комплексами захисту АС від несанкціонованого доступу, особливості технологій розслідування інцидентів безпеки;
- принципи управління програмними комплексами захисту АС від несанкціонованого доступу в інформаційних системах;
- основні типи, призначення та характеристики технологічних рішень, направлених на забезпечення управління програмними комплексами захисту АС від несанкціонованого доступу.

вміти:

- використовувати на практиці нормативні документи в галузі захисту інформації та міжнародні стандарти з управління програмними комплексами захисту АС від несанкціонованого доступу, Програмні комплекси захисту АС від несанкціонованого доступу, розуміти відмінності та переваги їх використання;
- реалізовувати організаційні та технічні завдання, які виникають в процесі проведення розслідування впровадження та забезпечення управління програмними комплексами захисту АС від несанкціонованого доступу.

та досягти наступних ***програмних результатів навчання:***

ПРз-1	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної та/або кібербезпеки; - вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; - виконувати аналіз реалізації прийнятої політики інформаційної та/або кібербезпеки;
ПРз-3	- вміти виявляти загрози проникнення або доступу зловмисників до таких мереж; - знати спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки безпроводових і мобільних мереж;

ПРз-5	- вміти проводити семантичний аналіз файлів; - вміти виявляти злоякісне програмне забезпечення й файли за їх структурою та поведінкою; вміти відновлювати пошкоджену інформацію; - вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ;
ПРз-8	- вміти організовувати процеси розслідування інцидентів у відповідності зі стандартами ISO 27001, ISO 20000, ISO/IEC TR 18044, NIST SP 800-61, CMU/SEI-2004-TR-015, ISO 27035, ISO 27037. ISO 27031; - - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах - проектувати та реалізувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; - вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах.

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	
Змістовий модуль 1. Програмні комплекси захисту АС від несанкціонованого доступу						
Тема 1. Введення в дисципліну. Основні терміни та визначення. Нормативно-правова база захисту АС від НСД	8	2				6
Тема 2. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу	24	2		6	6	10
Тема 3. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу	24	2		6	6	10
Тема 4. Базові програмні комплекси захисту АС від несанкціонованого доступу	56	6		8	12	30
Модульний контроль	8					
Семестровий контроль	30					
Усього	**150**	**12**		**20**	**24**	**56**

5. Програма навчальної дисципліни

Змістовий модуль 1. Програмні комплекси захисту АС від несанкціонованого доступу

Тема 1. Введення в дисципліну. Основні терміни та визначення. Нормативно-правова база захисту АС від НСД

Введення в дисципліну. Основні терміни та визначення. Нормативно-правова база захисту АС від НСД.

Тема 2. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу

Базові поняття. Побудова і структура критеріїв захищеності інформації.
Критерії конфіденційності: Довірча конфіденційність. Адміністративна конфіденційність. Повторне використання об'єктів. Аналіз прихованих каналів. Конфіденційність при обміні. Критерії цілісності: Довірча цілісність. Адміністративна цілісність. Відкат. Цілісність при обміні. Критерії доступності: Використання ресурсів. Стійкість до відмов. Гаряча заміна. Відновлення після збоїв. Критерії спостереженості: Реєстрація. Ідентифікація і автентифікація. Достовірний канал. Розподіл обов'язків. Цілісність комплексу засобів захисту. Самотестування. Ідентифікація і автентифікація при обміні. Автентифікація відправника. Автентифікація отримувача. Критерії гарантій: Архітектура. Середовище розробки. Послідовність розробки. Середовище функціонування. Документація. Випробування комплексу засобів захисту

Тема 3. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

Класифікація автоматизованих систем. Функціональні профілі захищеності. Визначення і призначення. Семантика профілю. Стандартні профілі. Стандартні функціональні профілі захищеності. Стандартні функціональні профілі захищеності для автоматизованих систем класу 1. Стандартні функціональні профілі для автоматизованих систем класу 2. Стандартні функціональні профілі захищеності для автоматизованих систем класу 3. Вибір профілю захищеності залежно від призначення автоматизованих систем. Стандартні функціональні профілі захищеності в КС, що входять до складу автоматизованих систем, призначених для автоматизації діяльності органів державної влади. Стандартні функціональні профілі захищеності КС, що входять до складу автоматизованих систем, які призначені для автоматизації банківської діяльності. Стандартні функціональні профілі захищеності в КС, що входять до складу автоматизованих систем, які призначені для керування технологічними процесами. Стандартні функціональні профілі захищеності в КС, що входять до складу довідково-пошукових систем. Відповідність правовим вимогам.

Тема 4. Базові програмні комплекси захисту АС від несанкціонованого доступу

Програмні комплекси захисту АС від несанкціонованого доступу. Система захисту інформації «ЛОЗА». Програмний комплекс засобів захисту інформації від несанкціонованого доступу "Гриф". Комплекс засобів захисту інформації від несанкціонованого доступу в інформаційно-телекомунікаційній системі«VTI-Рубіж». Комплекс засобів захисту інформації від несанкціонованого доступу OpenPGP. Аналіз типових проблем впровадження ПКЗ АС НСД.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, залік.
- *Комп'ютерного контролю:* програми - емулятори.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1	
		кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	6	6
Відвідування семінарських занять	1		
Відвідування практичних занять	1	10	10
Відвідування лабораторних занять	1	12	12
Робота на семінарському занятті	10		
Робота на практичному занятті	10	10	100
Лабораторна робота (в тому числі допуск, виконання, захист)	10	12	120
Виконання завдань для самостійної роботи	5	15	75
Виконання модульної роботи	25	4	100
Виконання ІНДЗ	30		
Максимальна кількість балів:		423	
Розрахунок коефіцієнта:		423/60=7,05	

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 для самостійної роботи студентів

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1			
1	Нормативно-правова база захисту АС від НСД	2	5
2	Структура критеріїв захищеності інформації НД ТЗІ.	4	5
3	Критерії конфіденційності НД ТЗІ.	4	5
4	Критерії цілісності НД ТЗІ.	4	5
5	Критерії доступності НД ТЗІ.	4	5
6	Критерії спостереженості НД ТЗІ.	4	5
7	Критерії гарантій НД ТЗІ.	4	5
8	Функціональні профілі захищеності НД ТЗІ.	4	5
9	Стандартні функціональні профілі захищеності НД ТЗІ.	4	5
10	Вибір профілю захищеності залежно від призначення автоматизованих систем.	4	5
11	Програмні комплекси захисту АС від несанкціонованого доступу.	4	5
12	Система захисту інформації «ЛОЗА».	4	5
13	Програмний комплекс засобів захисту інформації від несанкціонованого доступу "Гриф".	4	5
14	Комплекс засобів захисту інформації від несанкціонованого доступу в інформаційно-телекомунікаційній системі«VTI-Рубіж».	4	5
15	Відповідність програмних комплексів захисту АС від несанкціонованого доступу правовим вимогам.	2	5
	Разом	56	75

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв’язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – тест, що складається із 3-15 запитань. Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі екзамену, умовою допуску до якого є отриманням студентом 35 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Орієнтовний перелік питань для семестрового контролю

01 ВВЕДЕННЯ ВДИСЦИПЛІНУ. ОСНОВНІ ТЕРМІНИ ТА ВИЗНАЧЕННЯ. НОРМАТИВНО-ПРАВОВА БАЗА ЗАХИСТУ АС ВІД НСД

1. Основні терміни та визначення.
2. Нормативно-правова база захисту АС від НСД.

02 КРИТЕРІЇ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

3. Критерії конфіденційності.
4. Критерії цілісності.
5. Критерії доступності.
6. Критерії спостереженості.
7. Критерії гарантій.

03 КЛАСИФІКАЦІЯ АВТОМАТИЗОВАНИХ СИСТЕМ І СТАНДАРТНІ ФУНКЦІОНАЛЬНІ ПРОФІЛІ ЗАХИЩЕНОСТІ ОБРОБЛЮВАНОЇ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

1. Класифікація автоматизованих систем.
2. Функціональні профілі захищеності.
3. Стандартні функціональні профілі захищеності.
4. Вибір профілю захищеності залежно від призначення автоматизованих систем.

04 БАЗОВІ ПРОГРАМНІ КОМПЛЕКСИ ЗАХИСТУ АС ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

1. Система захисту інформації «ЛОЗА».
2. Програмний комплекс засобів захисту інформації від несанкціонованого доступу "Гриф".
3. Комплекс засобів захисту інформації від несанкціонованого доступу в інформаційно-телекомунікаційній системі«VTI-Рубіж».
4. Комплекс засобів захисту інформації від несанкціонованого доступу OpenPGP.

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: 150 год., лекції – 12 год., лабораторні заняття – 24 год., практичні заняття – 20 год., модульний контроль – 8 год., самостійна робота – 56 год.

Модулі (назви, бали)	**Змістовий модуль 1. Програмні комплекси захисту АС від несанкціонованого доступу (423 балів)**												
Лекції (теми, бали)	Введення в дисципліну. Основні терміни та визначення. Нормативно-правова база захисту АС від НСД (1 бал)	Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Ч1 (1 бал)	Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу Ч2 (1 бал)	Класифікація автоматизованих систем. Ч1 (1 бал)	Класифікація автоматизованих систем Ч2 (1 бал)	Базові програмні комплекси захисту АС від НСД. Ч1 (1 бал)	Базові програмні комплекси захисту АС від НСД. Ч2 (1 бал)						
Практичні, семінарські заняття (теми, бали)		Розробка критеріїв конфіденційності АС локального хоста (11 балів)	Розробка критеріїв цілісності АС локального хоста. (11 балів)	Розробка критеріїв доступності АС локального хоста (11 балів)	Розробка критеріїв спостереженості АС локального хоста (11 балів)	Розробка критеріїв гарантій АС локального хоста (11 балів)	Розробка функціонального профілю захищеності Г1 (11 балів)	Розробка функціонального профілю захищеності Г2 (11 балів)	Розробка функціонального профілю захищеності Г3 (11 балів)	Розробка функціонального профілю захищеності АС державної влади (11 балів)	Розробка функціонального профілю захищеності АС банку. (11 балів)		
Лабораторні заняття (теми, бали)		Розробка вимог до розгортання програмних комплексі захисту АС від НСД. (11 балів)	Вибір профілю захищеності залежно від призначення автоматизованих систем. (11 балів)	Розгортання системи захисту інформації «ЛОЗА». (11 балів)	Розробка нормативних документів на використання ПКЗ «ЛОЗА» (11 балів)	Розгортання ПКЗ захисту інформації від НСД "Гриф" (11 балів)	Розробка нормативних документів на використання ПКЗ "Гриф" (11 балів)	Розгортання ПКЗ захисту інформації від НСД «VTI-Рубіж» (11 балів)	Розробка нормативних документів на використання ПКЗ «VTI-Рубіж» (11 балів)	Комплекс засобів захисту інформації від несанкціонованого доступу OpenPGP (11 балів)	Розробка нормативних документів на використання OpenPGP (11 балів)	Аналіз відповідності ПКЗ АС від НСД нормативним вимогам (11 балів)	Аналіз функціонального профілі захищеності в КС, що входять до складу автоматизованих систем АСУ ТП (11 балів)
Самостійна робота	Самостійна робота (75 балів)												
Поточний контроль (вид, бали)	Модульна контрольна робота №1-4 (100 балів)												
Підсумковий контроль (вид, бали)	Екзамен (40 балів)												

8. Рекомендовані джерела

Основна (базова):

1. Закон України «Про основні засади забезпечення кібербезпеки України».
2. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"
3. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"
4. НД_2.5_004_99. Критерії оцінки захищеності інформації в комп'ютерних системах.
5. НД_2.5_005_99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності.
6. НД ТЗІ 1.1-003-99, «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», - 30с.
7. Андрєєв В.І., Хорошко В.О., Чередніченко В.С., Шелест М.Є., Основи інформаційної безпеки. Підручник. – К.: вид. ДУІКТ, 2009. –292 с.
8. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с.
9. Кобозева А.А., Мачалін І.О., Хорошко В.О., Аналіз захищеності інформаційних систем. Підручник. – К.: вид. ДУІКТ, 2010. - 316 с.
10. Прикладні аспекти аналізу та синтезу політик безпеки: навч. посіб. / В.А. Козачок, Н.В. Коршун, Н.П. Мазур, А.В. Платоненко, П.М. Складанний – К.: Київський університет імені Бориса Грінченка, 2021. – 267 с.
11. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
12. Цимбалюк В.С. Інформаційне право (теорія і практика). Монографія. – К.: 2009. - 364 с.

Допоміжна

1. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.
2. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
3. 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.
4. Єрмошин В.В., Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки. /Невойт Я.В., Єрмошин В.В.// Монографія. – К: ДУТ, 2015. – 124 С.
5. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум. Частина 1 – Комплекси засобів захисту інформації від НСД: навч. посіб. / М.В. Захарченко, В.Г. Кононович, В.Й. Кільдішев, Д.В. Голев // За ред. ак. МАІ М.В. Захарченка.– Одеса: ОНАЗ ім. О.С. Попова, 2011. – 168 с

9. Додаткові ресурси

1. CERT-UA: [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/.
2. Верховна Рада України. Законодавство України: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/
3. Державна служба спеціального зв'язку та захисту інформації: [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/index.
4. Програмний комплекс Засобів захисту інформації від НСД «Гриф». http://www.ict.com.ua/?lng=1&sec=8&art=51
5. Система захисту інформації ЛОЗА. http://avtoprom.kiev.ua/product.html/