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 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ: ПРОЕКТУВАННЯ, ВПРОВАДЖЕННЯ, СУПРОВІД»

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

2023 – 2024 навчальний рік

Розробник:

Платоненко Артем Вадимович, кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Платоненко Артем Вадимович, кандидат технічних наук, 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) Скаранний В.В. (ПІБ), «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	7 / 210		
Курс	4		
Семестр	7	8	
Кількість змістових модулів з розподілом:	3		
Обсяг кредитів	4	3	
Обсяг годин, в тому числі:	120	90	
Аудиторні	56	14	
Модульний контроль	8	2	
Семестровий контроль	30	30	
Самостійна робота	26	44	
Форма семестрового контролю		Екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Комплексні системи захисту інформації: проектування, впровадження, супровід» 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 навчальних планів спеціальності 125 Кібербезпека.

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 «Комплексні системи захисту інформації: проектування, впровадження, супровід» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Комплексні системи захисту інформації: проектування, впровадження, супровід» складається з трьох змістових модулів: Етапи проектування КСЗІ, Основні етапи впровадження КСЗІ, Організаційні заходи та супровід КСЗІ. Обсяг дисципліни – 210 год (7 кредитів).

Метою викладання навчальної дисципліни «Комплексні системи захисту інформації: проектування, впровадження, супровід» є отримання компетентностей зі створення комплексу системи захисту інформації на об’єктах інформаційної діяльності.

Завдання:

- надання студентам теоретичних знань про засоби і методи організаційного захисту інформації;
- формування у студентів категоріальних понять з принципів побудови КСЗІ;
- формування у студентів уміння аналізу ефективності КСЗІ;
- стимулювання студентів до активної аналітико-пошукової роботи, що спрямована на визначення ефективних шляхів застосування систем технічного захисту інформації.

Завдання полягає у формуванні теоретичних знань та практичних умінь у сфері побудови КСЗІ та набуття **наступних фахових компетентностей**:

КФ-7: Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

У результаті вивчення навчальної дисципліни формуються
загальні компетентності:

- ***компетентності у сфері навчання:***
  - здатність до організації самостійної навчальної, практичної та науково-дослідної діяльності;
- ***компетентності у сфері застосування знань в практичних ситуаціях***
  - вміння застосовувати здобуті теоретико-концептуальні професійні знання у процесі практичної роботи;

фахові компетентності:

- ***компетентності у сфері проектування політик безпеки:***
  - глибокі знання та розуміння принципів застосування КСЗІ, необхідного апаратного і організаційного забезпечення для їх впровадження;
  - уміння аналізувати створені та існуючі проекти КСЗІ;
  - здатність до самостійного створення КСЗІ;
- **компетентності у сфері науково-дослідної діяльності:**
  - уміння вивчати і систематизувати знання у галузі технічного захисту інформації;
  - вивчати, узагальнювати й упроваджувати на практиці організаційні засоби технічного захисту інформації.
- **компетентності у сфері вмінь працювати в групі:**
  - здатність використовувати навички взаємодії в роботі, компетентності у сфері навичок міжособистісного спілкування
  - здатність до продуктивного використання комунікації як складової професійної діяльності.

3. Результати навчання за дисципліною

При вивченні курсу «Комплексні системи захисту інформації: проектування, впровадження, супровід» студенти повинні

знати:

- історію та особливості розвитку систем технічного захисту інформації;
- основні процеси що вимагаються при впровадженні КСЗІ;
- класифікацію та характеристики апаратних засобів для ефективного впровадження КСЗІ;
- основні чинники, що визначають надійність і ефективність КСЗІ;
- понятійно-термінологічний апарат в області аналізу та впровадження КСЗІ;

уміти:

- визначати тип каналів витоку;
- аналізувати ефективність обраного засобу технічного захисту,
- виявляти особливості КСЗІ для різних типів задач;
- обґрунтовувати вибір технічних і організаційних засобів для ефективного впровадження КСЗІ;
- визначати ресурси, необхідні для забезпечення надійності функціонування КСЗІ з врахуванням факторів помилки у роботі користувачів.

та досягти наступних **програмних результатів навчання:**

ПРз-5	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної і кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - 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;
ПРз-7	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - здійснювати оцінку рівня захищеності інформації що обробляється в ІТС використовувати інструментальні засоби оцінювання наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих); - вирішувати задачі експертизи, випробування КСЗІ;

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	
СЕМЕСТР 7						
Змістовий модуль 1. Етапи проектування КСЗІ						
Тема 1. Поняття КСЗІ, призначення та функції.	8	2		2	2	2
Тема 2. Формування загальних вимог до КСЗІ.	8	2		2	2	2
Тема 3. Обґрунтування необхідності створення КСЗІ.	10	2		2	2	4
Тема 4. Обстеження середовищ функціонування.	16	4		4	4	4
Модульний контроль	4					
Разом за змістовим модулем 1	46	10		10	10	12
Змістовий модуль 2. Основні етапи впровадження КСЗІ						
Тема 5. Формування завдання на створення КСЗІ.	8	2		2	2	2
Тема 6. Розробка політики безпеки інформації.	10	2		2	2	4
Тема 7. Розробка технічного завдання на створення КСЗІ.	10	2		2	2	4
Тема 8. Розробка проекту КСЗІ.	12	2		2	4	4
Модульний контроль	4					
Разом за змістовим модулем 2	44	8		8	10	14

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт				
		Аудиторна:				Самостійна
		Лекції	Семінари	Практичні	Лабораторні	
Семестровий контроль (курсова робота)	30					
Разом за 7 семестр	120	18		18	20	26
СЕМЕСТР 8						
Змістовий модуль 3. Організаційні заходи та супровід КСЗІ						
Тема 9. Введення КСЗІ в дію та оцінка захищеності інформації. Супровід КСЗІ.	58	2		2	10	44
Модульний контроль	2					
Разом за змістовий модуль 3	60	2		2	10	44
Семестровий контроль	30					
Разом за 7 семестр	90	2		2	10	44
Усього годин	210	20		20	30	70

5. Програма навчальної дисципліни

7 СЕМЕСТР

Змістовий модуль 1. Етапи проектування КСЗІ.

Основні питання:

- Поняття КСЗІ, їх призначення та функції.
- Формування загальних вимог до КСЗІ.
- Обґрунтування необхідності створення КСЗІ.

Змістовий модуль 2. Основні етапи впровадження КСЗІ.

Основні питання:

- Обстеження середовищ функціонування.
- Формування завдання на створення КСЗІ.
- Розробка політики безпеки інформації.

8 СЕМЕСТР

Змістовий модуль 3. Організаційні заходи та супровід КСЗІ.

Основні питання:

- Розробка технічного завдання на створення КСЗІ.
- Розробка проекту КСЗІ.
- Введення КСЗІ в дію та оцінка захищеності інформації. Супроводження КСЗІ.

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 заняттях та семінарах, 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, екзамен.
- *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 та індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних та 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 у 7 та 8 семестрах

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	5	5	4	4	1	1
Відвідування практичних занять	1	5	5	4	4	1	1
Відвідування лабораторних	1	5	5	5	5	5	5
Робота на практичному занятті	10	5	50	4	40	1	10
Лабораторна робота (в тому числі допуск, виконання, захист)	10	5	50	5	50	5	50
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25	1	25
Виконання ІНДЗ	30						
Разом		-	145	-	133	-	97
Максимальна кількість балів: 375							
Розрахунок коефіцієнта: 375/60=6,25							

Модульний контроль здійснюється під час проведення модульної контрольної роботи з кожного модуля і визначається викладачем у балах контрольної модульної рейтингової оцінки.

Підсумковий контроль здійснюється за результатами підсумкової семестрової модульної рейтингової оцінки (суми підсумкових модульних оцінок) і заліку.

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
СЕМЕСТР 7		**26**	**10**
Змістовий модуль 1. Етапи проектування КСЗІ		12	5
1	Поняття КСЗІ, призначення та функції.	2	1
2	Формування загальних вимог до КСЗІ.	2	1
3	Обґрунтування необхідності створення КСЗІ.	4	2
4	Обстеження середовищ функціонування.	4	1
Змістовий модуль 2. Основні етапи впровадження КСЗІ		14	5
5	Формування завдання на створення КСЗІ.	2	1
6	Розробка політики безпеки інформації.	4	1
7	Розробка технічного завдання на створення КСЗІ.	4	2
8	Розробка проекту КСЗІ.	4	1
СЕМЕСТР 8		**44**	**5**
Змістовий модуль 3. Організаційні заходи та супровід КСЗІ		44	5
9	Введення КСЗІ в дію та оцінка захищеності інформації. Супроводження КСЗІ.	44	5

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 – письмова робота, що складається з 3 запитань. 1 та 2 питання – по 5 балів, 3 питання – 15 балів.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

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

Орієнтовний перелік питань для семестрового контролю

1. Надайте визначення інформаційної безпеки.
2. Надайте визначення загрози інформаційній безпеці.

3. Як поділяється інформація за режимом доступу до неї?
4. Які грифи таємності можуть надаватися інформації та який їх терміни дії?
5. Яка інформація не відноситься до державної таємниці?
6. Надайте визначення ТЗІ.
7. Які основні заходи з організації створення КСЗІ?
8. Який порядок проведення обстеження на об’єкті інформаційної діяльності?
9. Які розділи і підрозділи входять до складу технічного завдання на створення КСЗІ?
10. Які вимоги та функції висуваються до засобів антивірусного захисту?
11. Яка мета та порядок проведення обстеження та атестації виробництва?
12. Які заходи організовує та виконує виконавець робіт зі створення КСЗІ?
13. Які розділи містить технічне завдання на створення КСЗІ?
14. Який порядок розроблення та оформлення технічного завдання на створення КСЗІ?
15. Яка мета та порядок контролю за станом технічного захисту інформації?

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: 210 год., лекції –20 год., практичні заняття – 20 год., лабораторні – 30 год., модульний контроль – 10 год., самостійна робота – 70 год.

	Семестр 7								**Семестр 8**
Модулі (назви, бали)	**Змістовий модуль 1. Етапи проектування КСЗІ (145 балів)**				**Змістовий модуль 2. Основні етапи впровадження КСЗІ (133 бали)**				**Змістовий модуль3. Організаційні заходи та супровід КСЗІ (97 балів)**
Лекції (теми, бали)	№ 1 Поняття КСЗІ, призначення та функції (1 бал)	№ 2 Формування загальних вимог до КСЗІ. (1 бал)	№ 3 Обґрунтування необхідності створення КСЗІ. (1 бал)	№ 4-5 Обстеження середовищ функціонування. (2 бали)	№ 6 Формування завдання на створення КСЗІ. (1 бал)	№ 7 Розробка політики безпеки інформації. (1 бали)	№ 8 Розробка технічного завдання на створення КСЗІ. (1 бал)	№ 9 Розробка проекту КСЗІ. (1 бал)	№ 10 Введення КСЗІ в дію та оцінка захищеності інформації. Супроводження КСЗІ. (1 бал)
Практичні, заняття (теми, бали)	№ 1 Аналіз основних функцій КСЗІ (11 балів)	№ 2 Аналіз і оцінка загроз інформаційній безпеці (11 балів)	№ 3 Аналіз проблем викликаних для створення КСЗІ. (11 балів)	№ 4-5 Підготовка до обстеження об’єкта (22 бали)	№ 6 Визначення завдання захисту та моделі порушника (11 балів)	№ 7 Вивчення об’єкта на якому створюється КСЗІ (11 балів)	№ 8 Розробка ТЗ для вперше створених систем (11 балів)	№ 9 Ескізний проект, технічний проект, робочий проект (11 балів)	№ 10 Підготовка КСЗІ до введення в дію та подальші етапи впровадження (11 балів)
Лабораторні (теми, бали)	№ 1 Особливості функцій відповідно до об’єкта (11 балів)	№ 2 Описання вимог до КСЗІ (11 балів)	№ 3 Описання виявлених проблем та обґрунтування необхідності створення КСЗІ. (11 балів)	№ 4-5 Опис середовища функціонування (22 бали)	№ 6 Оформлення звіту про виконання робіт (11 балів)	№ 7 Оформлення політики безпеки (11 балів)	№ 8 Розробка ТЗ для модернізованих систем (11 балів)	№ 9-10 Визначення функцій КСЗІ по попередні технічні рішення (22 бали)	№ 11-15 Супроводження КСЗІ (55 балів)
Самостійна робота	Самостійна робота (5 балів)			Самостійна робота (5 балів)					Самостійна робота (5 балів)
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)			Модульна контрольна робота 2 (25 балів)					Модульна контрольна робота 3 (25 балів)
Підсумковий контроль (вид, бали)	Екзамен (40 балів)								

8. Рекомендовані джерела

Основна (базова):

1. Закон України "Про інформацію".
2. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".
3. Закон України "Про основи національної безпеки".
4. Постанова Кабінету Міністрів України від 27.11.1998 № 1893 «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію».
5. Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.
6. ДСТУ 33960-96 Захист інформації. Технічний захист інформації. Основні положення.
7. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
8. ДСТУ 33962-97 Захист інформації. Технічний захист інформації. Терміни та визначення;
9. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
10. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
11. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
12. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
13. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
14. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.
15. НД ТЗІ 1.6-004-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.
16. НД ТЗІ 1.6-005-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

Додаткова:

1. Хорошко В.О, Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки : К.: ДУІКТ, 2008. – 186 с.
2. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник. –К.: "МК-Прес", 2005. – 432 с.
3. “Безпека інформаційно-комунікаційних систем” в галузі знань “Інформаційна безпека”. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко, 2015. – 449 с.
4. Козачок В.А., Коршун Н.В., Мазур Н.П., Платоненко А.В., Складанний П.М. Прикладні аспекти аналізу та синтезу політик безпеки Навчальний посібник для студентів галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека – Київ: Вид-во КУБГ. 2021.-160 с.

9. Додаткові ресурси

1. Державна служба спеціального зв’язку та захисту інформації – Режим доступу: dsszzi.gov.ua
2. Офіційний портал Верховної ради України – Режим доступу: rada.gov.ua
3. Технічний захист інформації – Режим доступу: tzi.ua/ua/tz.html