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
«05» 09 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ПРИКЛАДНІ АСПЕКТИ АНАЛІЗУ ТА СИНТЕЗУ ПОЛІТИК БЕЗПЕКИ»

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 № 0526/22
_____ _____
(підпис) (прізвище, ініціали)
«___» _____ 2022

2022 – 2023 навчальний рік

Розробник:

Киричок Роман Васильович, доктор філософії з кібербезпеки, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Киричок Роман Васильович, доктор філософії з кібербезпеки, 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 _____ Павло СКЛАДАННИЙ

(підпис)

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

___.___. 2022 р.

Керівник освітньої програми _____ Артем ПЛАТОНЕНКО

(підпис)

Робочу програму перевірено

___.___. 2022 р.

Заступник декана _____ Євген ІВАНІЧЕНКО

(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	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4 / 120	
Курс	3	
Семестр	6	
Кількість змістових модулів з розподілом:	3	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	42	
Модульний контроль	6	
Семестровий контроль	30	
Самостійна робота	42	
Форма семестрового контролю	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Прикладні аспекти аналізу та синтезу політик безпеки» 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».

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 «Прикладні аспекти аналізу та синтезу політик безпеки» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Прикладні аспекти аналізу та синтезу політик безпеки» складається з трьох змістовних модулів: Основні засади створення політики інформаційної безпеки; Особливості попереднього етапу розробки політики інформаційної безпеки; Базові аспекти побудови та реалізації політики інформаційної безпеки. Обсяг дисципліни – 120 год. (4 кредитів).

Метою викладання навчальної дисципліни «Прикладні аспекти аналізу та синтезу політик безпеки» є:

– опанування загальними основами методології формування політики інформаційної безпеки;

– ґрунтовне ознайомлення студентів із основними нормативними документами щодо створення політики інформаційної безпеки та особливостями їх застосування на практиці;

– опанування навичками практичного використання та підтримки політик інформаційної безпеки в актуальному стані.

Завдання полягає у:

– наданні студентам базових теоретичних знань щодо формування політики інформаційної безпеки;

– стимулюванні студентів до активної аналітико-пошукової роботи, що спрямована на визначення найефективніших шляхів формування та застосування (реалізації) політик

інформаційної безпеки.

та набутті наступних ***фахових компетентносте:***

КФ-2	Здатність до використання інформаційно-комунікаційних та SMART-технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.
КФ-4	Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студенти повинні

знати:

– понятійно-термінологічний апарат в області аналізу та синтезу політик інформаційної безпеки;

– основні вітчизняні нормативні документи в галузі захисту інформації та міжнародні стандарти з інформаційної безпеки, процеси які висуваються ними при формуванні політики інформаційної безпеки, особливості підтвердження відповідності прийнятої політики;

– основні процеси формування та впровадження політики інформаційної безпеки;

– основні чинники, що визначають надійність і ефективність політик безпеки;

– основні типи, призначення та характеристики технологічних рішень, направлених на забезпечення ефективної реалізації політик інформаційної безпеки.

уміти:

– розробляти та визначати загальні принципи, завдання, вихідні дані та фактори, які необхідно врахувати при формування ефективної політики інформаційної безпеки;

– застосовувати національні та міжнародні стандарти при аналізі та розробленні політики інформаційної безпеки;

– здійснювати формування базових положень політики інформаційної безпеки, розробляти правила забезпечення інформаційної безпеки;

– здійснювати аналіз та оцінку ефективності впровадженої політики інформаційної безпеки;

– обґрунтовувати вибір технічних та програмних засобів задля ефективного впровадження політик інформаційної безпеки;

– визначати ресурси, необхідні для забезпечення надійності функціонування політик безпеки з врахуванням факторів помилки користувачів;

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

ПРз-1	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики безпеки інформаційної та/або кібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформації, інформаційно-комунікаційних (автоматизованих) та SMART-систем; - виконувати аналіз реалізації прийнятої політики інформаційної та/або кібербезпеки.
ПРз-4	- вирішувати задачі супроводу (в т.ч.: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-комунікаційних (автоматизованих) та SMART-системах; - реалізувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) та SMART-системах; - вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) та SMART-

	системах на основі моделей управління доступом (мандатних, дискреційних, рольових); - вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) та SMART-системах; - забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в IT та SMART-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	Індивідуальні	
Змістовий модуль 1. Основні засади створення політики інформаційної безпеки							
Тема 1. Вступ до НД «Прикладні аспекти аналізу та синтезу політик безпеки»	8	2	2	-			4
Тема 2. Нормативно-правова складова основ створення політики безпеки	12	4	2	-			6
Модульний контроль	2						
Разом	**22**	**6**	**4**	**0**			**10**
Змістовий модуль 2. Особливості попереднього етапу розробки політики інформаційної безпеки							
Тема 3. Технологія попереднього аудиту безпеки інформаційних ресурсів, як передумова формування політики безпеки	36	6	6	6			18
Модульний контроль	2						
Разом	**38**	**6**	**6**	**6**			**18**
Змістовий модуль 3. Базові аспекти побудови та реалізації політики інформаційної безпеки							
Тема 4. Особливості формування політик інформаційної безпеки організації	28	6	2	6			14
Модульний контроль	2						
Разом	**30**	**6**	**2**	**6**			**14**
Семестровий контроль	30						
Усього годин	**120**	**18**	**12**	**12**			**42**

5. Програма навчальної дисципліни

Змістовий модуль 1. Основні засади створення політики інформаційної безпеки

Тема 1. Вступ до НД «Прикладні аспекти аналізу та синтезу політик безпеки». Передумови необхідності застосування організаційних методів забезпечення безпеки інформації. Базові поняття політики інформаційної безпеки. Визначення основних причин та цілей створення політики безпеки.

Тема 2. Нормативно-правова складова основ створення політики безпеки. Основна група нормативно-правових документів, стандартів, що використовуються при формуванні політики безпеки. Міжнародний стандарт ISO/IEC 27002:2022 «Information security, cybersecurity and privacy protection – Information security controls». Комплексний міжнародний стандарт ISO 15408. Стандарт BSI (Німеччина) «Керівництво щодо захисту інформаційних технологій для базового рівня захищеності». Стандарт COBIT (Control Objectives for Information and related Technology). Функціональні критерії НД ТЗІ 2.5-004-99. Концептуальні підходи компаній IBM, Cisco Systems, Microsoft та інституту SANS.

Змістовий модуль 2. Особливості попереднього етапу розробки політики ІБ

Тема 3. Технологія попереднього аудиту безпеки інформаційних ресурсів, як передумова формування політики безпеки. Головні аспекти обстеження середовища функціонування інформаційно-комунікаційної системи та визначення об'єктів захисту. Інвентаризація інформаційних активів, як основний механізм визначення об'єктів захисту. Визначення та аналіз поняття загрози безпеці інформації. Основні підходи до формування моделі загроз. Підходи до формування моделі порушника. Особливості процедури проведення аналізу та оцінки ризиків ІБ.

Змістовий модуль 3. Базові аспекти побудови та реалізації політики інформаційної безпеки

Тема 4. Особливості формування політик інформаційної безпеки організації. Особливості організаційних аспектів формування політики безпеки. Розподіл функціональних обов'язків щодо забезпечення інформаційної безпеки в організації. Базові аспекти вироблення офіційної політики ІБ організації та окремих ключових керівництв. Базові аспекти вироблення процедур щодо попередження та реагування на порушення ІБ. Оптимізація сформованого плану забезпечення інформаційної безпеки організації.

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 семінарських та практичних 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, екзамен.

– *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.

6.1. Розрахунок рейтингових балів за видами поточного (модульного) контролю

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	3	3	3	3	3	3
Відвідування семінарських занять	1	2	2	3	3	1	1
Відвідування практичних занять	1	-	-	3	3	3	3
Відвідування лабораторних занять	1						
Робота на семінарському занятті	10	2	20	3	30	1	10
Робота на практичному занятті	10	-	-	3	30	3	30
Лабораторна робота (в тому числі допуск, виконання, захист)	10						
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		-	**55**	-	**99**	-	**77**
Максимальна кількість балів: 231							
Розрахунок коефіцієнта: 231/60=3,85							

6.2. 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 засади створення політики інформаційної безпеки		**10**	**5**
1	Вступ до НД «Прикладні аспекти аналізу та синтезу політик безпеки»	4	2
2	Нормативно-правова складова основ створення політики безпеки	6	3
Змістовий модуль 2. Особливості попереднього етапу розробки політики інформаційної безпеки		**18**	**5**

№ з/п	Назва теми	Кількість годин	Бали
3	Технологія попереднього аудиту безпеки інформаційних ресурсів, як передумова формування політики безпеки	18	5
Змістовий модуль 3. Базові аспекти побудови та реалізації політики інформаційної безпеки		**14**	**5**
4	Особливості формування політик інформаційної безпеки організації	14	5
	Разом	**42**	**15**

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**

6.3. 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 14 тестових завдань (відкритої та закритої форм). Модульна контрольна робота оцінюється у 25 балів.

6.4. 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.

Форма проведення екзамену – тестування в середовищі Moodle. Екзамен оцінюється у 40 балів (32 тестових завдання відкритої та закритої форм). Оцінювання результатів засвоєння теоретичних знань та оцінювання сформованості практичних навичок володіння цифровими технологіями студентами, продемонстровані на екзамені, представлене у таблиці.

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

6.5. Орієнтовний перелік питань для семестрового контролю

1. Передумови необхідності застосування організаційних методів забезпечення безпеки інформації.
2. Базові поняття політики інформаційної безпеки.
3. Визначення основних причин та цілей створення політики безпеки.
4. Основна група нормативно-правових документів, стандартів, що використовуються

при формуванні політики безпеки.

5. Міжнародний стандарт ISO/IEC 27002:2022 «Information security, cybersecurity and privacy protection – Information security controls».
6. Комплексний міжнародний стандарт ISO 15408.
7. Стандарт BSI (Німеччина) «Керівництво щодо захисту інформаційних технологій для базового рівня захищеності».
8. Стандарт COBIT (Control Objectives for Information and related Technology).
9. Функціональні критерії НД ТЗІ 2.5-004-99.
10. Концептуальний підхід компанії IBM.
11. Концептуальний підхід компанії Cisco Systems.
12. Концептуальний підхід компанії Microsoft.
13. Концептуальний підхід інституту SANS.
14. Головні аспекти обстеження середовища функціонування ІКС та визначення об’єктів захисту.
15. Інвентаризація інформаційних активів, як основний механізм визначення об’єктів захисту.
16. Визначення та аналіз поняття загрози безпеці інформації.
17. Основні підходи до формування моделі загроз.
18. Підходи до формування моделі порушника.
19. Поняття ризиків ІБ.
20. Основні способи оцінки інформаційних ризиків.
21. Організаційні аспекти формування політики безпеки.
22. Особливості процедури формування політики безпеки.
23. Основні аспекти вироблення офіційної політики ІБ підприємства.
24. Основні аспекти вироблення процедур для попередження порушення безпеки.
25. Організаційні аспекти щодо реакція на порушення безпеки.

6.6. 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: 120 год., лекції – 18 год., практичні заняття – 12 год., семінарські заняття – 12 год., модульний контроль – 6 год., семестровий контроль – 30 год., самостійна робота – 42 год.

Модулі (назви, бали)	**Змістовий модуль 1. Основні засади створення політики інформаційної безпеки (55 балів)**			**Змістовий модуль 2. Особливості попереднього етапу розробки політики інформаційної безпеки (99 балів)**			**Змістовий модуль 3. Базові аспекти побудови та реалізації політики інформаційної безпеки (77 бали)**		
Лекції (теми, бали)	Актуальність застосування в сучасних умовах інформатизації політики інформаційної безпеки та її базові поняття (1 бал)	Рекомендації міжнародних та національних стандартів щодо створенню політик безпеки (1 бал)	Кращі практики створення політик безпеки (1 бал)	Основні положення визначення об'єктів захисту (1 бал)	Базові принципи формування моделей загроз та порушника ІБ (1 бал)	Особливості процедури проведення аналізу та оцінки ризиків ІБ (1 бал)	Особливості організаційних аспектів формування політики безпеки (1 бал)	Базові аспекти вироблення офіційної політики ІБ організації (1 бал)	Базові аспекти вироблення процедур щодо попередження та реагування на порушення ІБ (1 бал)
Практичні заняття (теми, бали)				Визначення об'єктів захисту на основі обстеження середовища функціонування інформаційно-комунікаційної системи підприємства (11 балів)	Побудова моделей порушника та загроз безпеки інформації в інформаційно-комунікаційній системі підприємства (11 балів)	Основні аспекти проведення аналізу та кількісної оцінки ризиків інформаційної безпеки підприємства (11 балів)	Розподіл функціональних обов'язків щодо забезпечення інформаційної безпеки в організації (11 балів)	Формування загальної політик інформаційної безпеки організації та окремих ключових керівництв (11 балів)	Вироблення процедури реагування на порушення інформаційної безпеки (11 балів)
Семінарські заняття (теми, бали)	Світові тенденції розвитку ринку засобів захисту інформації (11 балів)	Аналіз сучасного нормативно-правового підгрунтя для формування політики інформаційної безпеки (11 балів)		Особливості обстеження обчислювальної системи, інформаційного та користувацького середовища підприємства (11 балів)	Особливості формалізація загроз та порушників інформаційної безпеки (11 балів)	Методики кількісної та якісної оцінки ризиків інформаційної безпеки організації (11 балів)			Оптимізація сформованого плану забезпечення інформаційної безпеки організації (11 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. Про інформацію: Закон України від 15.06.2022 № 2657-XII.
2. Про національну безпеку України: Закон України від 15.06.2022 № 2469-VIII.
3. Про захист інформації в автоматизованих системах: Закон України від 04.07.2020 № 80/94-ВР.
4. Про основні засади забезпечення кібербезпеки України: Закон України від 01.08.2022 № 2163-VIII.
5. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 01.07.2022 р. № 80/94-ВР.
6. Про державну таємницю: Закон України від 15.03.2022 №3855-XII.
7. Про доступ до публічної інформації: Закон України від 19.02.2022 № 2939-VI
8. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373.
9. Про затвердження Переліку службової інформації, що є власністю держави: Постанова МОН України від 18.03.2015 р. № v0319729-15
10. Цивільний кодекс України від 01.08.2022 р. № 435-IV.
11. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT)
12. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу». Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
13. НД ТЗІ 1.1-003-99, «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», - 30с.
14. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі». Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 53.
15. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.
16. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
17. НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розроблення технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі». Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
18. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
19. Андрєєв В.І., Хорошко В.О., Чередніченко В.С., Шелест М.Є., Основи інформаційної безпеки. Підручник. – К.: вид. ДУІКТ, 2009. –292 с.
20. Богуш В.М., Юдін О.К., Інформаційна безпека держави. –К.: «МК-Прес», 2005. – 432с.
21. Бурячок, В. Л. Основи інформаційної та кібернетичної безпеки / В. Бурячок, Р. Киричок, П. Складанний. – К. : Київський університет імені Бориса Грінченка, 2019. – 320 с. ISBN 978-966-676-281-1
22. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.
23. Березовська, І. Р. Адміністративно-правові засоби забезпечення інформаційної безпеки в Україні : дис. канд. юрид. Наук : 12.00.07 / І. Р. Березовська; М-во освіти і науки України, Нац. акад. внутр. справ України. - Київ, 2012. – 242 с.
24. Голубенко О.Л., Хорошко В.О., Петров О.С., Головань С.М., Яремчук Ю.Є., Політика інформаційної безпеки: підручник. – Луганськ: вид-во СНУ ім.. В.Даля, 2009, -300с.

25. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с.

26. Політика інформаційної безпеки: підручник / [О. Л. Голубенко, В. О. Хорошко, О. С. Петров, С. М. Головань, Ю.Є. Яремчук]. – Л. : вид-во СНУ ім. В.Даля, 2009. – 300 с.

27. Усач Б. Ф. Організація і методика аудиту: підручник / Б. Ф. Усач, З. О. Душко, М. М. Колос. - К.: Знання, 2006. - 295 с.

28. Єрмошин В.В., Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки. /Невойт Я.В., Єрмошин В.В.// Монографія. – К: ДУТ, 2015. – 124 С.

29. ISO/IEC 27002:2022 «Information security, cybersecurity and privacy protection – Information security controls», [Електронний ресурс] – Режим доступу: https://www.iso.org/standard/75652.html.

30. ISO/IEC 27007:2011 «Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems».

31. ISO/IEC 9001:2008 «Quality management systems. Requirements».

32. ISO/IEC 27006:2011 «Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems».

33. NIST 800-12 Rev.1 «An Introduction to Computer Security: The NIST Handbook», [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final.

34. NIST 800-18 Rev. 1 «Guide for Developing Security Plans for Federal Information Systems», [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-18/rev-1/final.

35. NIST 800-30 Rev.1 «Guide for Conducting Risk Assessments», [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

36. NIST 800-39 Rev.1 «Managing Information Security Risk: Organization, Mission, and Information System View», [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-39/final.

37. Alberts, C. J. Managing Information Security Risks: The OCTAVE Approach / C. J. Alberts, A J. Dorofee. Addison-Wesley, 2002. - 512 p.

38. IT Security Policy Management Usage Patterns Using IBM Tivoli Security Policy Manager / [Axel Buecker, Scott Andrews, Craig Forster, Nicholas Harlow, Ming Lu, Sridhar Muppidi, Trevor Norvill, Philip Nye, Günter Waller, Eric T. White]. - Publisher(s): IBM Redbook, 2011.

39. Network Security Policy: Best Practices White Paper [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/support/docs/availability/high-availability/13601-secpol.html

Додаткова:

1. Бем М.В. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник / М.В. Бем, І.М. Городиський, Г. Саттон, О.М. Родіоненко. – К.: К.І.С., 2015. – 220 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. Гребенніков, В.В. Комплексні системи захисту інформації: проектування, впровадження, супровід / В. Гребенніков. – М. : вид-во «Rídero», 2018. – 226 с. -ISBN 978-5-4493-1505-2

4. Кобозева А.А., Мачалін І.О., Хорошко В.О., Аналіз захищеності інформаційних систем. Підручник. – К.: вид. ДУІКТ, 2010. - 316 с.

5. Менеджмент інформаційної безпеки / [О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач та ін.]. – Чернігів. : ТПК «Орхідея», 2019. – 204 с.

9. Додаткові інформаційні ресурси

1. Верховна Рада України. Законодавство України: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/

2. Державна служба спеціального зв’язку та захисту інформації: [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/index.

3. Security Policy Templates [Електронний ресурс] – Режим доступу: https://www.sans.org/information-security-policy/