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 «СТАНДАРТИ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ»

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 № 0129/22
(підпис) (прізвище, ініціали)
«___» _____ 2022 р.

2022 – 2023 навчальний рік

Розробник:

Гулак Геннадій Миколайович, доктор технічних наук, доцент, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Гулак Геннадій Миколайович, доктор технічних наук, доцент, професор 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 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 № ___

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	2	
Семестр	3	
Кількість змістових модулів з розподілом:	2	
Обсяг кредитів	5	
Обсяг годин, в тому числі:	150	
Аудиторні	70	
Модульний контроль	10	
Семестровий контроль		
Самостійна робота	70	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Стандарти інформаційної та кібербезпеки» 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, 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 першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Стандарти інформаційної та кібербезпеки» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Стандарти інформаційної та кібербезпеки» складається з двох змістовних модулів. Обсяг дисципліни – 150 год. (5 кредитів).

Метою викладання навчальної дисципліни «Стандарти інформаційної та кібербезпеки» є вивчення кращих нормативно визначених практик забезпечення інформаційної та кібернетичної безпеки в організаціях різних форм власності; ґрунтовне ознайомлення студентів із основними нормативними документами в галузі інформаційної безпеки та особливостями їх застосування в майбутній професійної діяльності.

Завдання полягає у наданні студентам теоретичних знань і практичних умінь у галузі застосовування державних та міжнародних вимог, практик і стандартів та набуття наступних компетентностей:

Фахові компетентності:

КФ-1 – Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен

знати: основні державні нормативні документи в галузі захисту інформації та міжнародні стандарти з інформаційної безпеки, процеси які висуваються ними при побудові захищених систем, особливості підтвердження відповідності побудованого захисту; принципи побудови систем забезпечення інформаційної безпеки; основні типи, призначення та характеристики технологічних рішень, направлених на забезпечення інформаційної безпеки.

вміти: використовувати на практиці нормативно-правові акти в галузі захисту інформації, державні та міжнародні стандарти з інформаційної безпеки; реалізовувати організаційні та технічні завдання, які виникають в процесі побудови систем інформаційної безпеки.

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

ПРз-1 – готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної та/або кібербезпеки; розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; виконувати аналіз реалізації прийнятої політики інформаційної та/або кібербезпеки;

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.

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. Державне регулювання в сфері ІБК							
Тема 1. Теоретичні та методологічні основи захисту інформації, нормування ІКБ	18	4	6				8
Тема 2. Нормативно-правові акти про ІКБ і захист інформації	18	6	4				8
Тема 3. Державне регулювання діяльності у сфері ІКБ і захисту інформації	14	2	4	2			6
Тема 4. Забезпечення необхідних характеристик засобів захисту інформації	18	4	4				10

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Модульний контроль	6						
Разом	74	16	18	2			32
Змістовий модуль 2. Стандартизація методів, засобів і технологій ІБК							
Тема 5. Порядок і правила захисту інформації в комп'ютерних системах	20	4	4	2			10
Тема 6. Нормативно-правові акти про шифрування та цифровий підпис. Електронні довірчі послуги	20	4	4	2			10
Тема 7. Світовий досвід нормативного регулювання у сфері інформаційної та кібернетичної безпеки	16	2	4				10
Тема 8. Характеристика міжнародних стандартів в сфері ІБК	16	4	4				8
Модульний контроль	4						
Разом	76	14	16	4			38
Усього	**150**	**30**	**34**	**6**			**70**

5. Програма навчальної дисципліни

Змістовий модуль 1. Державне регулювання в сфері ІБК

Тема 1. Теоретичні та методологічні основи захисту інформації, нормування ІБК

Поняття про цілі і завдання стандартизації. Напрями стандартизації. Гармонізація міжнародних стандартів. Термінологічний апарат з питань інформаційної безпеки та кібербезпеки (ІБК). Захист інформації як складова ІБК та його основні методи. Характеристика інформації як предмета захисту. Інформація як об'єкт права власності. Сутність та цілі захисту інформації. Напрями стандартизації в сфері захисту інформації. Технічні регламенти.

Тема 2. Нормативно-правові акти про ІБК і захист інформації

Поняття про державну регуляторну політику. Повноваження державних органів в сфері ІБК. Загальна характеристика нормативно-правових актів з питань ІБК та захисту інформації. Захист інформації як об'єкт адміністративно-правового регулювання. Система органів регулювання технічного захисту інформації (ТЗІ). Організація криптографічного захисту інформації (КЗІ) в державі.

Тема 3. Державне регулювання діяльності у сфері ІБК і захисту інформації

Цілі та напрями реалізації державної політики у сфері захисту інформації. Ліцензування господарської діяльності у галузі захисту інформації. Дозвільна система проведення робіт у галузі ТЗІ. Поняття про органи спеціального зв'язку. Адміністративна відповідальність за порушення законодавства в сфері захисту інформації.

Тема 4. Забезпечення необхідних характеристик засобів захисту інформації

Етапи життєвого циклу засобів захисту інформації та їх характеристика. Критерії захищеності. Питання сертифікації продукції в сфері захисту інформації. Державна експертиза і оцінка відповідності у сфері захисту інформації. Світовий досвід сертифікації продукції у сфері захисту інформації на основі міжнародних стандартів.

Змістовий модуль 2. Стандартизація методів, засобів і технологій ІБК

Тема 5. Порядок і правила захисту інформації в комп'ютерних системах

Законодавство і нормативні документи (НД) про захист інформації в комп'ютерних системах. Класифікація автоматизованих систем в НД ТЗІ. Моделі захисту інформації в автоматизованій системі (АС). Модель порушника інформаційної безпеки. Порядок і правила захисту інформації в АС. Забезпечення конфіденційності, доступності й цілісності інформації в АС.

Тема 6. Нормативно-правові акти про шифрування та цифровий підпис, електронні довірчі послуги

Предмет криптографії. Криптосистеми та загрози їх безпеки. Симетричні та асиметричні криптосистеми. Формування та перевіряння цифрового підпису. Електронні довірчі послуги. Правила забезпечення криптографічного захисту інформації. Стандарти в криптографії.

Тема 7. Світовий досвід нормативного регулювання у сфері ІБК

Провідні світові та національні органи зі стандартизації. Нормативне регулювання у сфері інформаційної безпеки в ЄС. Підходи країн ЄС та НАТО щодо регулювання питань кібернетичної безпеки.

Тема 8. Характеристика міжнародних стандартів в сфері ІБК

Сімейство стандартів інформаційної та кібернетичної безпеки. Структура стандарту по кібербезпеці. Базові блоки стандарту ISO 27032. Заходи забезпечення кібербезпеки. Основи обміну інформацією та координації.

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	8	8	7	7
Відвідування семінарських занять	1	9	9	8	8
Відвідування практичних занять	1	1	1	2	2
Відвідування лабораторних занять	1				
Робота на семінарському занятті	10	9	90	8	80
Робота на практичному занятті	10	1	10	2	20
Лабораторна робота (в тому числі допуск, виконання, захист)	1				
Виконання завдань для самостійної роботи	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25
Виконання ІНДЗ	30				
Разом			148		147
Максимальна кількість балів:		295			
Розрахунок коефіцієнта:		295/100=2,95			

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. Державне регулювання в сфері ІБК			
1	Теоретичні та методологічні основи захисту інформації, нормування ІБК. Нормативно-правові акти про ІБК і захист інформації. Державне регулювання діяльності у сфері ІБК і захисту інформації. Забезпечення необхідних характеристик засобів захисту інформації: • виконання завдань відповідно до теми; • опрацювання фахових видань.	32	5
Змістовий модуль 2. Стандартизація методів, засобів і технологій ІБК			
2	Порядок і правила захисту інформації в комп'ютерних системах. Нормативно-правові акти про шифрування та цифровий підпис, електронні довірчі послуги. Світовий досвід нормативного регулювання у сфері ІБК. Характеристика міжнародних стандартів в сфері ІБК: • виконання завдань відповідно до теми; • опрацювання фахових видань.	38	5
	Разом	80	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 бали
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль, відповідно до навчального робочого плану, здійснюється шляхом виконання тестових контрольних робіт.

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 самоконтролю

1. Базові поняття у галузі інформаційної безпеки.
2. Складові інформаційної безпеки.
3. Характеристика інформації як предмета захисту.
4. Інформація як об'єкт права власності.
5. Сутність та цілі захисту інформації.
6. Циклічна модель інформаційної безпеки.
7. Потенційні загрози безпеки інформації та їх класифікація.
8. Загальна характеристика законодавчих актів в сфері захисту інформації.

9. Захист інформації як об’єкт адміністративно-правового регулювання.
10. Система органів регулювання технічного захисту інформації України.
11. Взаємодія суб’єктів системи технічного захисту інформації.
12. Напрями реалізації державної політики у сфері захисту інформації.
13. Ліцензування господарської діяльності у галузі захисту інформації.
14. Дозвільна система проведення робіт у галузі технічного захисту інформації.
15. Етапи життєвого циклу засобів захисту інформації та їх характеристика.
16. Сертифікації продукції і оцінка відповідності в сфері захисту інформації.
17. Державна експертиза у сфері захисту інформації.
18. Класифікація автоматизованих систем в НД ТЗІ.
19. Моделі захисту інформації в автоматизованій системі.
20. Модель порушника інформаційної безпеки.
21. Порядок і правила захисту інформації в АС.
22. Забезпечення конфіденційності, доступності й цілісності інформації в АС.
23. Криптосистеми та загрози їх безпеки.
24. Симетричні та асиметричні криптосистеми.
25. Формування та перевіряння електронного цифрового підпису.
26. Електронні довірчі послуги.
27. Порядок забезпечення криптографічного захисту інформації.
28. Провідні світові та національні органи зі стандартизації.
29. Нормативне регулювання у сфері інформаційної безпеки в ЄС.
30. Підходи країн ЄС та НАТО щодо регулювання питань кібернетичної безпеки.
31. Сімейство стандартів інформаційної та кібернетичної безпеки.
32. Структура стандарту по кібербезпеці.
33. Базові блоки стандарту ISO 27032.
34. Заходи забезпечення кібербезпеки.
35. Основи обміну інформацією та координації.

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 – 30 год., семінарські заняття – 34 год., практичні заняття – 6 год., самостійна робота – 70 год.

Модулі (назви, бали)	**Змістовий модуль 1. Державне регулювання в сфері ІБК (148 балів)**				**Змістовий модуль 2. Стандартизація методів, засобів і технологій ІБК (147 балів)**			
Лекції (теми, бали)	1-2. Теоретичні та методологічні основи ЗІ, нормування ІКБ (2 бали)	3-5. НПА про ІБК і захист інформації (3 бал)	6. Держ. регулювання діяльності у сфері ІКБ і ЗІ (1 бал)	7-8. Забезп. необхідних характеристик засобів ЗІ (2 бали)	9-10. Порядок і правила ЗІ в КС (2 бали)	11-12. НПА про шифрування та ЕЦП, ЕДП (2 бали)	13. Досвід нормативного регулювання у сфері ІБК (1 бал)	14-15. Характеристика міжнародних стандартів в сфері ІБК (2 бали)
Семінарські заняття (теми, бали)	Теоретичні та методологічні основи ЗІ, нормування ІКБ (33 бали)	НПА про ІБК і захист інформації (22 бали)	Держ. регулювання діяльності у сфері ІКБ і ЗІ (22 бали)	Забезп. необхідних характеристик засобів ЗІ (22 бали)	Порядок і правила ЗІ в КС (22 бали)	НПА про шифрування та ЕЦП, ЕДП (22 бали)	Досвід нормативного регулювання у сфері ІБК (22 бали)	Характеристика міжнародних стандартів в сфері ІБК (22 бали)
Практичні заняття (теми, бали)			Держ. регулювання діяльності у сфері ІКБ і ЗІ (11 балів)		Порядок і правила ЗІ в КС (11 балів)	НПА про шифрування та ЕЦП, ЕДП (11 балів)		
Самостійна робота	Самостійна робота (5 балів)				Самостійна робота (5 балів)			
Модульний контроль	Модульна контрольна робота 1 (25 балів)				Модульна контрольна робота 2 (25 балів)			
Підсумковий контроль (вид, бали)	Залік							

8. Рекомендовані джерела

Основна (базова):

1. Гулак Г.М., Жильцов О.Б., Складанний П.М., Киричок Р.В., Коршун Н.В. Інформаційна та кібернетична безпека підприємства / Навчальний підручник. КУБГ. – К. 2022. 451с.

Нормативно-правові акти

1. Закон України «Про стандартизацію», http://zakon.rada.gov.ua/
2. Закон України «Про технічні регламенти та оцінку відповідності», http://zakon.rada.gov.ua/
3. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України", http://zakon.rada.gov.ua/
4. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах", http://zakon.rada.gov.ua/
5. Закон України "Про електроні довірчі послуги", http://zakon.rada.gov.ua/
6. Закон України «Про інформацію», http://zakon.rada.gov.ua/
7. Закон України «Про захист персональних даних», http://zakon.rada.gov.ua/
8. Закон України «Про банки та банківську діяльність», http://zakon.rada.gov.ua/
9. Закон України «Про ліцензування видів господарської діяльності», http://zakon.rada.gov.ua/
10. Закон України «Про Національну систему конфіденційного зв’язку», http://zakon.rada.gov.ua/
11. Указ Президента України від 22.05.1998 №505 «Про Положення про порядок здійснення криптографічного захисту інформації в Україні», http://zakon.rada.gov.ua/
12. Указ Президента України від 27.09.1999 №1229 «Про Положення про технічний захист інформації в Україні», http://zakon.rada.gov.ua/
13. Указ Президента України від 26.08.2021 № 447/2021 «Про рішення Ради національної безпеки і оборони України від 27.01.2016 "Про Стратегію кібербезпеки України", http://zakon.rada.gov.ua/
14. Постанова Кабінету Міністрів № 373 Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, http://zakon.rada.gov.ua/
15. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису», http://zakon.rada.gov.ua/
16. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.
17. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розроблення технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
18. 33. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
19. 34. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.
20. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.
21. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.
22. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

23. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.
24. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розроблення технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
25. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.
26. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу.
27. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
28. Положення про державну експертизу в сфері технічного захисту інформації. Затверджене наказом ДСТСЗІ СБ України від 29.12.1999 №62 і зареєстроване в Міністерстві юстиції України 24.01.2000 за №40/4261
29. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб. Затверджене наказом ДСТСЗІ СБ України від 23.02.2002 № 9 і зареєстроване в Міністерстві юстиції України 13.03.2002 за № 245/6533
30. Стандарт ISO/IEC 27001:2013 «Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги».
31. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT).
32. ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ і загальна модель (ISO/IEC 15408-1:2009, IDT)
33. ДСТУ ISO/IEC 15408-2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги (ISO/IEC 15408-2:2008, IDT)
34. ДСТУ ISO/IEC 15408-3:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантій безпеки (ISO/IEC 15408-3:2008, IDT)
35. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування і перевірка
36. ДСТУ 7624:2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блочного перетворення
37. ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція хешування
38. ДСТУ ГОСТ 28147-2009. Системи обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення
39. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення
40. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт
41. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення
42. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення
43. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва
44. ДБН 2.2-3-2004 Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.

Допоміжна

1. 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.
2. Єрмошин В.В., Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки. /Невойт Я.В., Єрмошин В.В.// Монографія. – К: ДУТ, 2015. – 124 С.
3. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.

9. Додаткові 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. CERT-UA: [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/.