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
«01» 09 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ОСНОВИ ІНФОРМАЦІЙНОЇ І КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ»

для студентів

спеціальності	125 Кібербезпека та захист інформації
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 № 0633/23
(підпис) (прізвище, ініціали)
«___» _____ 2023 р.

2023 – 2024 навчальний рік

Розробники:

Складанний Павло Миколайович, кандидат технічних наук, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Складанний Павло Миколайович, кандидат технічних наук, завідувач 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.М. (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	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4 / 120	
Курс	1	
Семестр	1	
Кількість змістових модулів з розподілом:	4	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	56	
Модульний контроль	8	
Семестровий контроль	-	
Самостійна робота	56	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Основи інформаційної і кібербезпеки та захисту інформації» 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, освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем.

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

Програма визначає обсяги знань, якими повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Основи інформаційної і кібербезпеки та захисту інформації» та необхідне методичне забезпечення, складові і технологію

Навчальна дисципліна «Основи інформаційної і кібербезпеки та захисту інформації» складається з чотирьох змістових модулів: Загальні поняття про інформацію, інформаційний і кіберпростори, безпеку, події та інциденти безпеки, Структура та стислий опис сучасних кібератак. Загальні поняття про організацію захисту від їх деструктивного впливу, Тенденції впровадження сучасних цифрових технологій в системи безпеки критично важливих об'єктів інфраструктури. Поняття стратегії безпеки КВОІ, Інтернет речей – як об'єкт критичної інфраструктури. Тенденції розвитку та перспективи захисту IoT-пристроїв у світі. Обсяг дисципліни – 120 год. (4 кредити).

Метою викладання навчальної дисципліни «Основи інформаційної і кібербезпеки та захисту інформації» є:

- вивчення основних підходів до забезпечення інформаційної безпеки в організаціях різної форми власності;
- ґрунтовне ознайомлення студентів із основними нормативними документами 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 знань 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

та ***набуття наступних фахових компетентностей***:

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.
КФ-2	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.
КФ-3	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ-4	Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

3. Результати навчання за дисципліною

При вивченні курсу «Основи інформаційної і кібербезпеки та захисту інформації» студенти повинні

знати:

- основні вітчизняні 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 нормативні документи в галузі захисту інформації та міжнародні стандарти з інформаційної безпеки, розуміти відмінності побудованих відповідно до їх вимог систем;
- реалізовувати організаційні та технічні завдання, які виникають в процесі побудови систем інформаційної безпеки.

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	
Змістовий модуль 1. Загальні поняття про інформацію, інформаційний і кіберпростори, безпеку, події та інциденти безпеки						
Тема 1. Загальні поняття про інформацію, інформаційний і кіберпростори, безпеку, події та інциденти безпеки	22	8			4	10
Модульний контроль	2					
Разом	**24**	**8**			**4**	**10**
Змістовий модуль 2. Структура та стислий опис сучасних кібератак. Загальні поняття про організацію захисту від їх деструктивного впливу						
Тема 2. Структура та стислий опис сучасних кібератак. Загальні поняття про організацію захисту від їх деструктивного впливу	22	8			4	10
Модульний контроль	2					
Разом	**24**	**8**			**4**	**10**
Змістовий модуль 3. Тенденції впровадження сучасних цифрових технологій в системи безпеки критично важливих об'єктів інфраструктури. Поняття стратегії безпеки КВОІ						
Тема 3. Тенденції впровадження сучасних цифрових технологій в системи безпеки критично важливих об'єктів інфраструктури. Поняття стратегії безпеки КВОІ	22	8			4	10
Модульний контроль	2					
Разом	**24**	**8**			**4**	**10**
Змістовий модуль 4. Інтернет речей – як об'єкт критичної інфраструктури. Тенденції розвитку та перспективи захисту IoT-пристроїв у світі						
Тема 4. Інтернет речей – як об'єкт критичної інфраструктури. Тенденції розвитку та перспективи захисту IoT-пристроїв у світі	20	6			4	10
Тема 5. Україна в умовах сучасних кіберзагроз: концептуальний підхід до формування систем	26	6			4	16

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт				
		Аудиторна:				Самостійна
		Лекції	Семінари	Практичні	Лабораторні	
інформаційної і кібербезпеки та захисту інформації						
Модульний контроль	2					
Разом	**48**	**12**			**8**	**26**
Усього разом	**120**	**36**			**20**	**56**

5. Програма навчальної дисципліни

Змістовий модуль 1. Основи інформаційної та кібернетичної безпеки та захисту інформації

Тема 1. Загальні поняття про інформацію, інформаційний і кіберпростори, безпеку, події та інциденти безпеки

Базові поняття у галузі інформаційної безпеки. Складові інформаційної безпеки. Характеристика інформації як предмета захисту. Інформація як об'єкт права власності. Сутність та цілі захисту інформації. Циклічна модель інформаційної безпеки. Потенційні загрози безпеки інформації та їх класифікація.

Змістовий модуль 2. Структура та стислий опис сучасних кібератак. Загальні поняття про організацію захисту від їх деструктивного впливу

Тема 2. Структура та стислий опис сучасних кібератак. Загальні поняття про організацію захисту від їх деструктивного впливу

Загальна характеристика законодавчих актів в сфері захисту інформації. Захист інформації як об’єкт адміністративно-правового регулювання. Система органів регулювання технічного захисту інформації України. Взаємодія суб’єктів системи технічного захисту інформації.

Змістовий модуль 3. Тенденції впровадження сучасних цифрових технологій в системи безпеки критично важливих об’єктів інфраструктури. Поняття стратегії безпеки КВОІ

Тема 3. Тенденції впровадження сучасних цифрових технологій в системи безпеки критично важливих об’єктів інфраструктури. Поняття стратегії безпеки КВОІ

Напрями реалізації державної політики у сфері захисту інформації. Ліцензування господарської діяльності у галузі захисту інформації. Дозвільна система проведення робіт у галузі технічного захисту інформації.

Змістовий модуль 4. Інтернет речей – як об’єкт критичної інфраструктури. Тенденції розвитку та перспективи захисту IoT-пристроїв у світі

Тема 4. Інтернет речей – як об’єкт критичної інфраструктури. Тенденції розвитку та перспективи захисту IoT-пристроїв у світі

Етапи життєвого циклу засобів захисту інформації та їх характеристика. Питання сертифікації продукції в сфері захисту інформації. Державна експертиза у сфері захисту інформації.

Тема 5. Україна в умовах сучасних кіберзагроз: концептуальний підхід до формування систем інформаційної і кібербезпеки та захисту інформації

Класифікація автоматизованих систем в НД ТЗІ. Моделі захисту інформації в автоматизованій системі. Модель порушника інформаційної безпеки. Порядок і правила захисту інформації в КС/АС. Забезпечення доступності й цілісності інформації в АС.

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.

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, екзамен.
- *Комп'ютерного контролю:* тестові програми.
- *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		Модуль 3		Модуль 4	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	4	4	4	4	4	4	6	6
Відвідування семінарських занять	1								
Відвідування практичних занять	1								
Відвідування лабораторних занять	1	2	2	2	2	2	2	4	4
Робота на семінарському занятті	10								
Робота на практичному занятті	10								
Лабораторна робота (в тому числі допуск, виконання, захист)	10	2	20	2	20	2	20	4	40
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25	1	25	1	25
Виконання ІНДЗ	30								
Разом		-	56	-	56	-	56	-	80
Максимальна кількість балів: 248									
Розрахунок коефіцієнта: 248/100=2,48									

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. Загальні поняття про інформацію, інформаційний і кіберпростори, безпеку, події та інциденти безпеки		10	5
1	Складові інформаційної безпеки ● виконання завдань відповідно до теми; ● опрацювання фахових видань.	10	5
Змістовий модуль 2. Структура та стислий опис сучасних кібератак. Загальні поняття про організацію захисту від їх деструктивного впливу		10	5
2	Захист інформації як об’єкт адміністративно-правового регулювання ● виконання завдань відповідно до теми; ● опрацювання фахових видань.	10	5
Змістовий модуль 3. Тенденції впровадження сучасних цифрових технологій в системи безпеки критично важливих об’єктів інфраструктури. Поняття стратегії безпеки КВОІ		10	5
3	Модель порушника інформаційної безпеки ● виконання завдань відповідно до теми; ● опрацювання фахових видань.	10	5

Змістовий модуль 4. Інтернет речей – як об'єкт критичної інфраструктури. Тенденції розвитку та перспективи захисту IoT-пристроїв у світі		26	5
4	Криптосистеми та загрози їх безпеки : ● виконання завдань відповідно до теми; ● опрацювання фахових видань.	26	5
	Разом	56	20

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, обгрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – комп'ютерний тест, що складається 20 запитань закритої та відкритої форм.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

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

Орієнтовний перелік питань для самоперевірки

1. Надайте визначення наступним поняттям: «кібернетичний простір», «Інтернет», «Всесвітня павутина», «веб-браузер».
2. Опишіть основні складові кіберпростору.
3. Виділіть три рівні кібернетичного простору.
4. Що виконує служба доменних імен?
5. Назвіть основні функції веб-браузерів.
6. Перерахуйте та опишіть основні компоненти веб-браезера.
7. Назвіть три рівні адресації в комп'ютерних мережах, та наведіть приклади адрес до кожного з рівнів.
8. Поясніть, що таке MAC-адреса, та опишіть її структуру.
9. Опишіть структуру IP-адреси та поясніть що таке маска підмережі і для чого вона використовується?
10. Назвіть основні критерії віднесення IP-адреси до певного класу мережі.
11. Назвіть та опишіть IP-адреси спеціального призначення.
12. Поясніть, що таке служба DNS?
13. Поясніть, що таке протокол DHCP?
14. Для чого призначена утиліта ipconfig?
15. Назвіть основне призначення утиліти ping та опишіть алгоритм її роботи.
16. Пакетами якого мережевого протоколу є echo-пакети команди ping?
17. Назвіть основну відмінність утиліт ping та traceroute.

18. Поясніть, що таке сервіс Whois?
19. Що таке гіпертекст у сучасному розумінні та назвіть основні його елементи?
20. Надайте визначення наступним поняттям: «сайт» та «web-сторінка».
21. Що таке копірайтинг та які основні цілі переслідуються при формуванні інформаційного наповнення сайту?
22. Опишіть структуру інтернет-ресурсу.
23. Назвіть основні шаблони поведінки користувача в кіберпросторі.

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 – 36 год., лабораторні роботи – 20 год., модульний контроль – 8 год., самостійна робота – 56 год.

Модулі (назви, бали)	**Змістовий модуль 1. (56 балів)**		**Змістовий модуль 2. (56 балів)**		**Змістовий модуль 3. (56 балів)**	**Змістовий модуль 4. (56 балів)**	
Лекції (теми, бали)	Загальні поняття про інформацію, інформаційний і кіберпростори, безпеку, події та інциденти безпеки (4 бали)		Структура та стислий опис сучасних кібератак. Загальні поняття про організацію захисту від їх деструктивного впливу (4 бали)		Тенденції впровадження сучасних цифрових технологій в системи безпеки критично важливих об'єктів інфраструктури. Поняття стратегії безпеки КВОІ (4 бали)	Інтернет речей – як об'єкт критичної інфраструктури. Тенденції розвитку та перспективи захисту IoT-пристроїв у світі (3 бали)	Україна в умовах сучасних кіберзагроз: концептуальний підхід до формування систем інформаційної і кібербезпеки та захисту інформації (3 бали)
Лабораторні заняття (теми, бали)	Кібернетичний простір та доступ до системи WWW за допомогою веб-браузера (11 балів)	Фізична основа кіберпростору – Інтернет. Мережеві утиліти та їх використання для моніторингу та діагностики мережі (11 балів)	Інтернет-комерція та її вплив на соціум (11 балів)	Основи інформаційно-пошукових систем (11 балів)	Основи інформаційно-пошукових систем (22 бали)		Основи віртуалізації в комп'ютерних системах (44 бали)
Самостійна робота	Самостійна робота (5 балів)		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)	Модульна контрольна робота 4 (25 балів)	

8. Рекомендовані джерела

Базова

1. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с.
2. НД ТЗІ 1.1-003-99, «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу», – 30с.
3. Богуш В.М., Юдін О.К. Інформаційна безпека держави. –К.: «МК-Прес», 2005. – 432с.
4. Цимбалюк В.С. Інформаційне право (теорія і практика). Монографія. – К.: 2009. – 364 с.
5. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ, 2015. – 288 с.
6. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем. Підручник. – К.: вид. ДУІКТ, 2010. – 316 с.
7. Андрєєв В.І., Хорошко В.О., Чередніченко В.С., Шелест М.Є. Основи інформаційної безпеки. Підручник. – К.: вид. ДУІКТ, 2009. –292 с.
8. Закон України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI // Відомості Верховної Ради України. – 2011. – № 16. – с. 93.
9. Закон України «Про інформацію» // Відомості Верховної Ради, 1992, № 48, с. 650 – 651.
10. Закон України «Про державну таємницю» від 21.01.1994 // Відомості Верховної Ради України. – 1994. – № 16. – с. 93.
11. Закон України «Про основи національної безпеки України» // Урядовий кур’єр, 30 липня 2003 р.
12. Закон України «Про захист інформації в автоматизованих системах» // Відомості Верховної Ради України, 1994. - № 31. – С. 286.
13. Постанова Верховної Ради України від 16 січня 1997 року N 3/97-ВР «Про затвердження Концепції національної безпеки України»
14. Постанова Кабінету Міністрів України «Про затвердження Концепції технічного захисту інформації в Україні» від 08.10.1997 р.
15. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
16. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
17. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
18. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).
19. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT)
20. ДСТУ ISO 19011:2012 Настанови щодо здійснення аудитів систем управління (ISO 19011:2011, IDT).
21. ISO/IEC TR 27019:2013 Information technology — Security techniques — Information security management guide lines based on ISO/IEC 27002 for process control systems specific to the energy utility industry (Інформаційні технології. Методи захисту. Настанова щодо менеджменту інформаційної безпеки на основі ISO/IEC 27002 для систем керування процесами в індустрії енергетичних сервісних програм).
22. ДСТУ IEC/TS 62351-1:2014 Керування енергетичними системами та пов'язаний з ним інформаційний обмін. Безпека даних та комунікацій. Частина 1. Безпека зв'язку мережі та системи. Загальні положення (IEC/TS 62351-1:2007, IDT).
23. Закон України «Про ліцензування господарської діяльності» // Відомості Верховної Ради (ВВР), 2015, № 23, ст.158.
24. Указ Президента України «Про деякі заходи з дерегулювання підприємницької діяльності» від 23.07.1998 № 817.

25. Постанова Кабінету Міністрів України від 18.05.2011 року №517 «Про затвердження переліку послуг у галузі технічного захисту інформації, господарська діяльність щодо надання яких підлягає ліцензуванню».
26. Постанова Кабінету Міністрів України від 25.05.2011 року №543 «Про затвердження переліків послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та криптосистем і засобів криптографічного захисту інформації, господарська діяльність щодо яких підлягає ліцензуванню».
27. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб. Наказ ДСТСЗІ СБ України від 23.02.2002 № 9.
28. Бекірова Е. Правова природа інституту ліцензування певних видів господарської діяльності // Підприємництво, господарство і право. – 2007, №10, с. 95 - 97.
29. Господарський кодекс України: Коментар. – Х.: «Одіссей», 2004. – 848 с.

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. 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. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.

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