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
«___»_____ 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ОСНОВИ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ»

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 № 1975/22
(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	вибіркова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	5 / 150	
Курс	4	
Семестр	8	
Кількість змістових модулів з розподілом:	2	
Обсяг кредитів	5	
Обсяг годин, в тому числі:	150	
Аудиторні	56	
Модульний контроль	8	
Семестровий контроль	30	
Самостійна робота	56	
Форма семестрового контролю	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Основи захисту конфіденційних даних» 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 «Основи захисту конфіденційних даних» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Основи захисту конфіденційних даних» складається з двох змістовних модулів: Базові принципи формування ефективної системи захисту конфіденційної інформації; Технологічні аспекти побудови ефективної системи захисту конфіденційних даних. Обсяг дисципліни – 150 год. (5 кредитів).

Метою викладання навчальної дисципліни «Основи захисту конфіденційних даних» є:

– ґрунтовне ознайомлення студентів із основними нормативно-правовими документами в галузі захисту конфіденційної інформації та особливостями їх застосування на практиці;

– опанування загальними основами методології створення та аналізу різноманітних типових технологій побудови ефективних систем захисту конфіденційних даних;

– ознайомлення з основними підходами та технологічними рішеннями направленими на забезпечення захисту конфіденційних даних з урахуванням сучасних досягнень та розвитку інформаційних технологій;

– опанування навичками проектування, впровадження та супроводу комплексних систем моніторингу та попередження витоку конфіденційних даних.

Завдання полягає у:

– формуванні у студентів усвідомлення важливості захисту конфіденційної інформації в загальній структурі забезпечення кібербезпеки;

– наданні студентам базових теоретичних знань у галузі захисту конфіденційної інформації;

– набутті студентами практичних навичок застосування сучасних технологій створення ефективних систем попередження витоку конфіденційних даних та їх експлуатації;

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

КФ-11	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-комунікаційних (автоматизованих) та SMART-систем згідно встановленої політики інформаційної та/або кібербезпеки.
КФ-12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної та/або кібербезпеки.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студенти повинні

знати:

– загальні засади правового регулювання захисту конфіденційної інформації;

– основи забезпечення правового режиму конфіденційної інформації;

– основні вітчизняні нормативні документи в галузі захисту конфіденційної інформації та міжнародні стандарти з інформаційної безпеки, процеси які висуваються ними при побудові захищених систем, особливості підтвердження відповідності побудованого захисту;

– принципи побудови систем моніторингу та попередження витоку конфіденційних даних.

уміти:

– розробляти та визначати загальні принципи побудови ефективної системи моніторингу та попередження витоку конфіденційних даних, завдання, вихідні дані та фактори, які необхідно врахувати при проектуванні комплексного захисту конфіденційної інформації;

– здійснювати аналіз та оцінку параметрів комплексної системи моніторингу та попередження витоку конфіденційних даних;

– здійснювати аналіз архітектурної структури і взаємозв’язків елементів комплексної системи захисту конфіденційних даних: формувати опис та середовища функціонування структурних компонентів такої системи, визначати склад потрібного апаратного та програмного забезпечення, здійснювати аналіз необхідних технологій обробки інформації;

– здійснювати оцінку ефективності, як окремих компонентів, так і в цілому всієї системи захисту конфіденційних даних;

– застосовувати національні та міжнародні стандарти при аналізі та розробленні комплексної системи захисту конфіденційних даних та (або) її елементів;

– застосовувати типові підходи до проектування та налагодження сучасного комплексу систем захисту конфіденційних даних, здійснити порівняння підходів до організації типових архітектур таких комплексів;

– оцінювати ефективність впровадження перспективних засобів і систем моніторингу та попередження витоку інформації, що використовується при створенні комплексної системи захисту конфіденційних даних;

– використовувати на практиці нормативні документи в галузі захисту конфіденційної 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 комплексної системи захисту конфіденційних даних;

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

ПРз-8	- вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-комунікаційних (автоматизованих) та SMART-системах; - проводити розслідування інцидентів інформаційної та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної та/або кібербезпеки; - забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації.
ПРз-9	- забезпечувати неперервність бізнес процесів організації на базі системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів; - забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісної та якісної оцінки.
ПРз-12	- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-комунікаційних (автоматизованих) та SMART-системах; - аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в IT та SMART-системах; - аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

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. Базові принципи формування ефективної системи захисту конфіденційної інформації							
Тема 1. Особливості комплексного захисту конфіденційної інформації	28	4			10		14
Тема 2. Організаційно-правовий рівень забезпечення безпеки конфіденційних даних	18	2		2	6		8
Модульний контроль	4						
Разом	**50**	**6**		**2**	**16**		**22**
Змістовий модуль 2. Технологічні аспекти побудови ефективної системи захисту конфіденційних даних							
Тема 3. Розмежування, контроль доступу до інформації, як основний рубіж захисту від несанкціонованого отримання конфіденційних даних	20	4		4	2		10
Тема 4. Організація захисту циркулюючих в комп'ютерних мережах конфіденційних даних	10	2		2			6

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Тема 5. Основні технології моніторингу та попередження витоку конфіденційних даних	36	2		10	6		18
Модульний контроль	4						
Разом	**70**	**8**		**16**	**8**		**34**
Семестровий контроль	30						
Усього годин	**150**	**14**		**18**	**24**		**56**

5. Програма навчальної дисципліни

Змістовий модуль 1. Базові принципи формування ефективної системи захисту конфіденційної інформації

Тема 1. Особливості комплексного захисту конфіденційної інформації. Характеристика конфіденційної інформації, як підвиду інформації з обмеженим доступом. Основні загрози та дії, що призводять до втрати конфіденційної інформації. Канали несанкціонованого отримання конфіденційної інформації. Методи несанкціонованого отримання конфіденційної інформації. Комплексний підхід до побудови системи захисту від загроз порушення конфіденційності інформації.

Тема 2. Організаційно-правовий рівень забезпечення безпеки конфіденційних даних. Нормативно-правові засади забезпечення безпеки конфіденційної інформації. Основні організаційні аспекти забезпечення захисту конфіденційних даних. Особливості інформаційно-аналітичної робота у контексті забезпечення захисту конфіденційної інформації.

Змістовий модуль 2. Технологічні аспекти побудови ефективної системи захисту конфіденційних даних

Тема 3. Розмежування, контроль доступу до інформації, як основний рубіж захисту від несанкціонованого отримання конфіденційних даних. Ключові поняття розмежування та контролю доступу до інформаційних ресурсів. Основні механізми контролю доступу до інформаційних ресурсів автоматизованої системи. Особливості побудови та функціонування систем ідентифікації/аутентифікації. Розмежування доступу, як складова частина системи управління доступом до інформаційних ресурсів. Особливості дискреційного, мандатного та рольового управління доступом. Поняття про моделювання розмежування доступу.

Тема 4. Організація захисту циркулюючих в комп'ютерних мережах конфіденційних даних. Технології забезпечення захисту конфіденційних даних, що передаються комп'ютерними мережами. Особливості мережевої ідентифікації/аутентифікації. Основні мережеві протоколи ідентифікації/автентифікації. Технологічні аспекти реалізації механізму єдиного входу (Single Sign-On). Забезпечення захисту конфіденційних даних з використанням технології віртуальних приватних мереж (VPN).

Тема 5. Основні технології моніторингу та попередження витоку конфіденційних даних. Загальні основи технологій моніторингу та попередження витоку конфіденційних даних. Сучасні механізми боротьби з витоком корпоративних конфіденційних даних. Технологічні аспекти забезпечення контролю зовнішнього периметру корпоративної мережі. Прикладні основи технологій моніторингу подій та управління інцидентами інформаційної 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:* 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 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.

6.1. 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	3	3	4	4
Відвідування семінарських занять	1				
Відвідування практичних занять	1	1	1	8	8
Відвідування лабораторних занять	1	8	8	4	4
Робота на семінарському занятті	10				
Робота на практичному занятті	10	1	10	8	80
Лабораторна робота (в тому числі допуск, виконання, захист)	10	8	80	4	40
Виконання завдань для самостійної роботи	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25
Виконання ІНДЗ	30				
	Разом	**-**	**132**	**-**	**166**
Максимальна кількість балів: 298					
Розрахунок коефіцієнта: 298/60=4,97					

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. Базові принципи формування ефективної системи захисту конфіденційної інформації		**22**	**5**
1	Особливості комплексного захисту конфіденційної інформації	14	3
2	Організаційно-правовий рівень забезпечення безпеки конфіденційних даних	8	2
Змістовий модуль 2. Технологічні аспекти побудови ефективної системи захисту конфіденційних даних		**34**	**5**
3	Розмежування, контроль доступу до інформації, як основний рубіж захисту від несанкціонованого отримання конфіденційних даних	10	1
4	Організація захисту циркулюючих в комп'ютерних мережах конфіденційних даних	6	1
5	Основні технології моніторингу та попередження витоку конфіденційних даних	18	3
	Разом	**56**	**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 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. Характеристика конфіденційної інформації як підвиду інформації з обмеженим доступом.
2. Основні загрози та дії що призводять до втрати конфіденційної інформації.
3. Канали несанкціонованого отримання конфіденційної інформації.
4. Методи несанкціонованого отримання конфіденційної інформації.
5. Комплексний підхід до побудови системи захисту від загроз порушення конфіденційності інформації.
6. Нормативно-правові засади забезпечення безпеки конфіденційної інформації.
7. Створення власних нормативно-правових документів організації.
8. Основні організаційні аспекти забезпечення захисту конфіденційних даних.
9. Методи роботи з персоналом.
10. Політика інформаційної безпеки.
11. Процес реалізації організаційних заходів.
12. Особливості інформаційно-аналітичної робота у контексті забезпечення захисту конфіденційної інформації.
13. Ключові поняття розмежування та контролю доступу до інформаційних ресурсів.
14. Основні механізми контролю доступу до інформаційних ресурсів автоматизованої системи.
15. Особливості побудови та функціонування систем ідентифікації/аутентифікації.
16. Парольні системи ідентифікації/аутентифікації.
17. Апаратна ідентифікація/аутентифікація.
18. Біометричні методи ідентифікації/аутентифікації.
19. Розмежування доступу, як складова частина системи управління доступом до інформаційних ресурсів.
20. Концепція ізолювання автоматизованої системи для роботи з конфіденційною інформацією.
21. Особливості дискреційного управління доступом.
22. Особливості мандатного управління доступом.
23. Особливості рольового управління доступом.
24. Поняття про моделювання розмежування доступу.
25. Модель Харрісона-Руззо-Ульмана.
26. Модель Белла-ЛаПадули.
27. Технологія виявлення та попередження витоку конфіденційних даних.
28. Методи розпізнавання конфіденційної інформації.
29. Базові компоненти DLP-систем та їх характеристика.
30. Інтелектуалізовані механізми виявлення та попередження витоку конфіденційних

даних.

31. Технологія забезпечення захисту зовнішнього периметру.

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: 150 год., лекції – 14 год., практичні заняття – 18 год., лабораторні заняття – 24 год., модульний контроль – 8 год., семестровий контроль – 30 год., самостійна робота – 56 год.

Модулі (назви, бали)	**Змістовий модуль 1. Базові принципи формування ефективної системи захисту конфіденційної інформації (132 балів)**				**Змістовий модуль 2. Технологічні аспекти побудови ефективної системи захисту конфіденційних даних (166 бали)**						
Лекції (теми, бали)	Конфіденційна інформація як об'єкт захисту (1 бал)	Комплексний підхід щодо організації ефективної системи попередження витоку конфіденційної інформації (1 бал)	Основи організаційно-правового та інформаційно-аналітичного забезпечення безпеки конфіденційних даних (1 бал)		Особливості контролю доступу до інформаційних ресурсів АС (1 бал)		Основні методи та моделі розмежування доступу до інформаційних ресурсів АС (1 бал)	Технології забезпечення захисту конфіденційних даних, що передаються комп'ютерними мережами (1 бал)	Загальні основи технологій моніторингу та попередження витоку конфіденційних даних (1 бал)		
Лабораторні заняття (теми, бали)	Ідентифікація інформаційних активів та класифікація конфіденційної інформації на підприємстві (33 бали)	Оцінка доступності конфіденційної інформації для зловмисників (22 бали)	Аналітичне дослідження інфраструктури домену безпеки, як превентивний механізм запобігання витоку конфіденційної інформації (11 балів)	Можливості компрометації реквізитів доступу користувачів (22 бали)			Побудова та аналіз формалізованої моделі системи розмежування доступу домена безпеки структурного підрозділу підприємства (11 балів)		Дослідження ефективності механізму боротьби з витоком корпоративних конфіденційних даних (11 балів)		Дослідження ефективності механізмів забезпечення контролю зовнішнього периметру, моніторингу подій та управління інцидентами ІБ (22 бали)
Практичні заняття (теми, бали)			Формування загальної моделі захисту конфіденційних даних підприємства (11 балів)		Побудова захищеного домену безпеки структурного підрозділу підприємства на базі Windows AD (11 балів)	Впровадження базової двохфакторної аутентифікації користувачів в домені безпеки з використанням USB-ключа (11 балів)		Технології забезпечення мережевої аутентифікації та організації віддаленого робочого столу (11 балів)	Організація механізму боротьби з витоком корпоративних конфіденційних даних (11 балів)	Технологічні аспекти забезпечення контролю зовнішнього периметру корпоративної мережі (22 бали)	Прикладні основи технологій моніторингу подій та управління інцидентами ІБ (22 бали)
Самостійна робота	Самостійна робота (5 балів)				Самостійна робота (5 балів)						
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)				Модульна контрольна робота 2 (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 Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 12.09.2009 р. № 505/98.
9. Про електронні документи та електронний документообіг: Закон України від 22.05.03 р. № 851-IV.
10. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373.
11. Про затвердження переліку послуг у галузі технічного захисту інформації, господарська діяльність щодо надання яких підлягає ліцензуванню: Постанова Кабінету Міністрів України від 18.05.2011 року №517.
12. Про затвердження Переліку службової інформації, що є власністю держави: Постанова МОН України від 18.03.2015 р. № v0319729-15
13. Цивільний кодекс України від 01.08.2022 р. № 435-IV.
14. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT)
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», - 30с.
17. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
18. Андрєєв В.І., Хорошко В.О., Чередніченко В.С., Шелест М.Є., Основи інформаційної безпеки. Підручник. – К.: вид. ДУІКТ, 2009. –292 с.
19. 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.
20. 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.
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. Береза А. Електронна комерція: Навч. посібник / Київський національний економічний ун- т. — Київ.: КНЕУ, 2002. — 326с.
24. 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.

25. Брижко В., Новицький А., Цимбалюк В., Швець М. Електронна комерція: правові заходи та заходи удосконалення: монографія / Науково-дослідний центр правової інформатики Академії правових наук України. — Київ.: НДЦПІ АПрНУ, 2008. — 149с.

26. 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

27. Гулак Г.М. Основи криптографічного захисту інформації: підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук, Вінниц. нац. техн. ун-т.– Вінниця : ВНТУ, 2012.– 199 с.

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

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

30. Мухачов В.А. Методи практичної криптографії: посібник / Мухачов В.А., Хорошко В.А. К.: ООО «ПоліграфКонсалтинг», 2005. – 215 с.

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

32. Пількевич, І. А. Захист інформації в автоматизованих системах управління : навч. посіб. / І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

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

34. Янчева Л. Електронна комерція: організація та облік: навч.посіб. / Харківський держ. ун-т харчування та торгівлі. — Харків. : ХДУХТ, 2008. — 231с.

35. RFC 3281. An Internet Attribute Certificate Profile for Authorization [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc3628

36. RFC 3379. Delegated Path Validation and Delegated Path Discovery Protocol Requirements [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc3379

37. RFC 5750 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling

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

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

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

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

42. Badger, M. Zenoss Core Network and System Monitoring / M. Badger. -Birmingham: Packt Publising, 2008. 261 p.

43. Cheswick, W.R. Firewalls and Internet Security: Repelling the Wily Hacker / W.R. Cheswick, S.M. Bellovin, A.D. Rubin. 2nd ed. - Addison-Wesley, 2003.-455 p.

44. Neumann P.G. Practical Architectures for survivable Systems and Networks. Technical Report. - SRI International: Computer Science Laboratory, 2001. - 209 pp. - http://www.csl.sri.com/neumann/survivability.dvi.

45. Schubert, M. Nagios 3 Enterprise Network Monitoring / M. Schubert, D. Bennett, J. Gines. Syngress, 2008. - 338 p.

46. West-Brown, M.J. Handbook for Computer Security Incident Response Teams (CSIRTs) / M.J. West-Brown, D. Stikvoort, K.P. Kossakowski. -Pittsburgh: Carnegie Mellon Software Engineering Institute, 2003. 201 p.

Додаткова:

1. Бабенко Т.В. Криптологія в тестах, задачах і прикладах: навч. посібник/ Т.В. Бабенко, Г.М. Гулак, С.О. Сушко, Л.Я. Фомічова. – Д.: Національний гірничий університет, 2013, - 318с.

2. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К.: ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.

3. Богуш В.М. Криптографічні застосування елементарної теорії чисел: посібник / Богуш В.М., Мухачов В.А. - К.: вид. ДУІКТ, 2006. – 126с

4. Богуш В.М., Юдін О.К., Інформаційна безпека держави. –К.: «МК-Прес», 2005. – 432с.

5. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування: монографія / І.Д. Горбенко, Ю.І. Горбенко; Харк. нац. ун-т радіоелектрон., ЗАТ «Ін-т інформ. Технологій». – Харків.: Форт, 2012. – 868 с.

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

7. Цимбалюк В.С. Інформаційне право (теорія і практика). Монографія. – К.: 2009. – 364с.

8. ISO/IEC 15408-1: Information technology. Security techniques - Evaluation criteria for IT security, Part 1: Introduction and general model, 1999.

9. ISO/IEC 15408-2: Information technology. Security techniques - Evaluation criteria for IT security, Part 2: Security functional requirements, 1999.

10. ISO/IEC 15408-3: Information technology. Security techniques - Evaluation criteria for IT security, Part 3: Security assuracce requirements, 1999. ISO/IEC 17799: Information technology - Code of practice for Information security management, 2000.

11. ISO/IEC 7498-2. Information processing systems Open Systems Interconnection Basic Reference Model. Part 2: Security Architecture. Switzeland, 1989. 32 pp.

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. CIS Benchmarks: кращі практики, гайдлайни і рекомендації з інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/company/pentestit/blog/338532/

4. Incident Response Platform: The Road to Automating IR [Електронний ресурс] // Офіційний сайт компанії Cynet. – Режим доступу : https://www.cynet.com/ incident-response-services/incident-response-platform-theroad-to-automating-ir/