Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-педагогічної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«___»_____ 2024 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕХНОЛОГІЇ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ БЕЗПЕКИ»

для студентів

спеціальності	125 Кібербезпека та захист інформації
освітнього рівня	другого (магістерського)
освітньої програми	125.00.02 Безпека інформаційних і комунікаційних систем

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307986
Програма № 3359/24
Начальник відділу моніторингу якості освіти
(підпис) (прізвище, ініціали)
«___» _____ 20 24 р.

2023 – 2024 навчальний рік

Розробник:

Козачок Валерій Анатолійович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Козачок Валерій Анатолійович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 01.09.2022 р. № 12

Завідувач кафедри _____ (підпис) Павло СКЛАДАННИЙ

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.02 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.

Керівник освітньої програми ___ (підпис) Володимир СОКОЛОВ

Робочу програму перевірено

___.___. 2022 р.

Заступник декана _____ (підпис) Євген ІВАНІЧЕНКО

Пролонговано:

на 2023/2024 н.р. _____ (підпис) Складанний П.В. (ПІБ), «23» 08 2023 р., протокол № 8

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	6 / 180	
Курс	5	
Семестр	10	
Кількість змістових модулів з розподілом:	1	
Обсяг кредитів	6	
Обсяг годин, в тому числі:	180	
Аудиторні	48	
Модульний контроль	12	
Семестровий контроль	-	
Самостійна робота	120	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Технології розслідування інцидентів 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 другого (магістерського) 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 другого (магістерського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Технології розслідування інцидентів безпеки» та необхідне методичне забезпечення, складові і технологію.

Навчальна дисципліна «Технології розслідування інцидентів безпеки» складається з одного змістового модулю: Технології розслідування інцидентів безпеки. Обсяг дисципліни – 180 год. (6 кредитів).

Метою викладання навчальної дисципліни «Технології розслідування інцидентів безпеки» є:

- вивчення основних підходів до забезпечення інформаційної безпеки в організаціях різної форми власності;
- ґрунтовне ознайомлення студентів із основними технологіями розслідування інцидентів безпеки 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 і практичних знань при розслідуванні інцидентів 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.

Фахові компетентності навчальної дисципліни:

КФ-1	Здатність до застосування сучасних інформаційних і 4ез пекових технологій у сфері захисту інформації.
КФ-5	Здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен

знати:

- основні вітчизняні нормативні документи в галузі захисту інформації та міжнародні стандарти з інформаційної безпеки, процеси які формалізуються ними при управлінні інцидентами інформаційної безпеки, особливості технологій розслідування інцидентів безпеки;
- принципи управління інцидентами інформаційної безпеки в інформаційних системах;
- основні типи, призначення та характеристики технологічних рішень, направлених на забезпечення управління інцидентами інформаційної безпеки.

вміти:

- використовувати на практиці нормативні документи в галузі захисту інформації та міжнародні стандарти з управління інцидентами інформаційної безпеки, технології розслідування інцидентів безпеки, розуміти відмінності та переваги їх використання;
- реалізовувати організаційні та технічні завдання, які виникають в процесі проведення розслідування інцидентів безпеки та забезпечення управління інцидентами 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; - вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; - виконувати аналіз реалізації прийнятої політики інформаційної та/або кібербезпеки;
ПРз-3	- вміти виявляти загрози проникнення або доступу зловмисників до таких мереж; - знати спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки безпроводових і мобільних мереж;
ПРз-5	- вміти проводити семантичний аналіз файлів; - вміти виявляти злоякісне програмне забезпечення й файли за їх структурою та поведінкою; вміти відновлювати пошкоджену інформацію; - вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ;

ПРз-8	- вміти організовувати процеси розслідування інцидентів у відповідності зі стандартами ISO 27001, ISO 20000, ISO/IEC TR 18044, NIST SP 800-61, CMU/SEI-2004-TR-015, ISO 27035, ISO 27037. ISO 27031; - - 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. Технології розслідування інцидентів безпеки							
Тема 1. Введення в дисципліну. Основні терміни та визначення. Нормативно-правова база розслідування інцидентів безпеки	32	2					30
Тема 2. Керівництво з реагування на інциденти	42	4		4	4		30
Тема 3. Інструменти розслідування інцидентів інформаційної безпеки	50	6		6	8		30
Тема 4. Управління інцидентами інформаційної безпеки.	44	4		6	4		30
Модульний контроль	12						
Усього	**180**	**16**		**16**	**16**		**120**

5. Програма навчальної дисципліни

Змістовий модуль 1. Технології розслідування інцидентів безпеки

Тема 1. Введення в дисципліну. Основні терміни та визначення. Нормативно-правова база розслідування інцидентів безпеки

Базові поняття технологій управління інцидентами інформаційної безпеки у галузі інформаційної безпеки. Життєвий цикл атаки. Реагування на інциденти інформаційної безпеки . Основні етапи процесу реагування на інциденти інформаційної безпеки. Алгоритми аналізу подій. Інструменти реагування на інциденти інформаційної безпеки.

Тема 2. Керівництво з реагування на інциденти

Базові поняття технологій управління інцидентами інформаційної безпеки у галузі інформаційної безпеки. Життєвий цикл атаки. Реагування на інциденти інформаційної безпеки. Основні етапи процесу реагування на інциденти інформаційної безпеки. Інструменти реагування на інциденти інформаційної безпеки.

Тема 3. Інструменти розслідування інцидентів інформаційної безпеки

Інструменти розслідувань інцидентів інформаційної безпеки: Autopsy, Encrypted Disk Detector, Wireshark, Magnet RAM Capture, Network Miner, NMAP, RAM Capturer, Forensic Investigator, FAW, HashMyFiles, USB Write Blocker, Crowd Response, NFI Defraser, ExifTool, Toolsley, SIFT, Dumpzilla, Browser History, ForensicUserInfo, Back Track, Paladin, Sleuth Kit. Криміналістичний аналіз інцидентів інформаційної безпеки.

Тема 4. Управління інцидентами інформаційної безпеки.

Основні поняття. Етап планування і підготовки. Етап виявлення і звітності. Етап реагування. Етап оцінки і прийняття рішення. Етап реагування. Етап засвоєних уроків.

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 змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульної контрольної роботи 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	
		кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	8	8
Відвідування семінарських занять	1		
Відвідування практичних занять	1	8	8
Відвідування лабораторних занять	1	8	8
Робота на семінарському занятті	10		
Робота на практичному занятті	10	8	80
Лабораторна робота (в тому числі допуск, виконання, захист)	10	8	80
Виконання завдань для самостійної роботи	5	8	40
Виконання модульної роботи	25	6	150
Максимальна кількість балів:		374	
Розрахунок коефіцієнта:		374/100=3,74	

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 для самостійної роботи студентів

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1			
1	Введення в дисципліну. Основні терміни та визначення. Нормативно-правова база розслідування інцидентів безпеки.	30	10
2	Керівництво з реагування на інциденти.	30	10
3	Інструменти розслідування інцидентів інформаційної безпеки.	30	10
4	Управління інцидентами інформаційної безпеки.	30	10
	Разом	120	40

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв’язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – тест, що

складається із 3-15 запитань. Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

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

Орієнтовний перелік питань для самоконтролю

01 НОРМАТИВНО-ПРАВОВА БАЗА РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ БЕЗПЕКИ

1. Базові поняття технологій управління інцидентами.
2. Життєвий цикл атаки.
3. Реагування на інциденти інформаційної безпеки .
4. Основні етапи процесу реагування на інциденти інформаційної безпеки.
5. Алгоритми аналізу подій.
6. Інструменти реагування на інциденти інформаційної безпеки.

02 КЕРІВНИЦТВО З РЕАГУВАННЯ НА ІНЦИДЕНТИ

1. Політики інформаційної безпеки.
2. Організація інформаційної безпеки.
3. Безпека людських ресурсів.
4. Управління ресурсами СУІБ.
5. Контроль доступу.
6. Фізична безпека та безпека інфраструктури.
7. Безпека експлуатації.
8. Безпека комунікацій.
9. Придбання.
10. Керівництво по використанню розроблення та підтримка інформаційних систем.
11. Взаємовідносини з постачальниками.
12. Управління інцидентами інформаційної безпеки.
13. Аспекти інформаційної безпеки управління безперервністю бізнесу.
14. Відповідність правовим вимогам.

03 ІНСТРУМЕНТИ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1. Керівництво по використанню Autopsy.
2. Керівництво по використанню Encrypted Disk Detector.
3. Керівництво по використанню Wireshark.
4. Керівництво по використанню Magnet RAM Capture.
5. Керівництво по використанню Network Miner.
6. Керівництво по використанню NMAP.
7. Керівництво по використанню RAM Capturer.
8. Керівництво по використанню Forensic Investigator.
9. Керівництво по використанню FAW.
10. Керівництво по використанню HashMyFiles.
11. Керівництво по використанню USB Write Blocker.
12. Керівництво по використанню Crowd Response.
13. Керівництво по використанню NFI Defraser.
14. Керівництво по використанню ExifTool.
15. Керівництво по використанню Toolsley.
16. Керівництво по використанню SIFT.
17. Керівництво по використанню Dumpzilla.
18. Керівництво по використанню Browser History.
19. Керівництво по використанню ForensicUserInfo.
20. Керівництво по використанню Back Track.
21. Керівництво по використанню Paladin.
22. Керівництво по використанню Sleuth Kit.

23. Криміналістичний аналіз інцидентів інформаційної безпеки.

04 УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1. Основні поняття управління інцидентами інформаційної безпеки.
2. Етап планування і підготовки.
3. Етап виявлення і звітності.
4. Етап реагування.
5. Етап оцінки і прийняття рішення.
6. Етап засвоєних уроків.

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: 180 год., лекції – 16 год., лабораторні заняття – 16 год., практичні заняття – 16 год., модульний контроль – 12 год., самостійна робота – 120 год.

Модулі (назви, бали)	Змістовий модуль 1. Технології розслідування інцидентів безпеки (374 бали)							
Лекції (теми, бали)	Введення в дисципліну. Основні терміни та визначення. Нормативно-правова база розслідування інцидентів безпеки (1 бал)	Керівництво з реагування на інциденти Ч1 (1 бал)	Керівництво з реагування на інциденти Ч2 (1 бал)	Інструменти розслідування інцидентів інформаційної безпеки Ч1 (1 бал)	Інструменти розслідування інцидентів інформаційної безпеки Ч2 (1 бал)	Інструменти розслідування інцидентів інформаційної безпеки Ч3 (1 бал)	Управління інцидентами інформаційної безпеки. Ч1 (1 бал)	Управління інцидентами інформаційної безпеки. Ч2 (1 бал)
Практичні, семінарські заняття (теми, бали)		Базові поняття технологій управління інцидентами інформаційної безпеки у галузі інформаційної безпеки. (11 балів)	Реагування на інциденти інформаційної безпеки. (11 балів)	Безпека експлуатації (11 балів)	Безпека комунікацій (11 балів)	Організація інформаційної безпеки. (11 балів)	Управління інцидентами інформаційної безпеки (22 бали)	Аспекти інформаційної безпеки управління безперервністю бізнесу (11 балів)
Лабораторні заняття (теми, бали)		Життєвий цикл атаки. (11 балів)	Інструменти реагування на інциденти інформаційної безпеки. (22 бали)	Аналіз інцидентів з використанням Autopsi . (11 балів)	Аналіз інцидентів з використанням Encrypted Dssk Detector. (11 балів)	Аналіз інцидентів з використанням Wsreshark (11 балів)	Аналіз інцидентів з використанням Forensic Investigator (11 балів)	Аналіз інцидентів з використанням FAW (11 балів)
Самостійна робота	Самостійна робота (40 балів)							
Поточний контроль (вид, бали)	Модульні контрольні роботи №1-6 (150 балів)							
Підсумковий контроль (вид, бали)	Залік							

8. Рекомендовані джерела

Основна (базова):

1. Закон України "Про інформацію".
2. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".
3. Закон України "Про основи національної безпеки".
4. Закон України «Про основні засади забезпечення кібербезпеки України».
5. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"
6. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"
7. НД ТЗІ 1.1-003-99, «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу», - 30с.
8. ISO 15489-1 Інформація та документація. Керування записами. Частина 1. Загальні положення
9. ISO 22301 Соціальна безпека. Системи управління безперервністю бізнесу. Вимоги
10. ISO 22313 Соціальна безпека. Системи управління безперервністю бізнесу. Настанова
11. ISO/IEC 11770-1 Інформаційні технології. Методи захисту. Керування ключами. Частина 1. Основні положення
12. ISO/IEC 11770-2 Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних алгоритмів
13. ISO/IEC 11770-3 Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних алгоритмів
14. ISO/IEC 20000-1 Інформаційні технології. Керування послугами. Частина 1. Вимоги до системи керування послугами
15. ISO/IEC 20000-21) Інформаційні технології. Керування послугами. Частина 2. Настанови щодо застосування систем керування послугами
16. ISO/IEC 27001 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги
17. ISO/IEC 27005 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки
18. ISO/IEC 27007 Інформаційні технології. Методи захисту. Настанови для аудиту систем управління інформаційною безпекою
19. ISO/IEC 27031 Інформаційні технології. Методи захисту. Настанови для інформаційних і телекомунікаційних технологій стосовно готовності до забезпечення безперервності бізнесу
20. ISO/IEC 27033-1 Інформаційні технології. Методи захисту. Безпека мережі. Частини 1. Огляд та концепції
21. ISO/IEC 27033-2 Інформаційні технології. Методи захисту. Безпека мережі. Частина 2. Настанови щодо проектування та впровадження безпеки мереж
22. ISO/IEC 27033-3 Інформаційні технології. Методи захисту. Безпека мережі. Частина 3. Рекомендовані сценарії мереж. Загрози, методи проектування та заходи безпеки
23. ISO/IEC 27033-4 Інформаційні технології. Методи захисту. Безпека мережі. Частина 4. Убезпечення міжмережевих комунікацій з використанням шлюзів безпеки
24. ISO/IEC 27033-5 Інформаційні технології. Методи захисту. Безпека мережі. Частина 5. Убезпечення комунікацій в мережах з використанням віртуальної приватної мережі (VPNs)
25. ISO/IEC 27035 Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки
26. ISO/IEC 27036-1 Інформаційні технології. Методи захисту. Інформаційна безпека для взаємовідносин з постачальниками. Частина 1. Огляд та концепції
27. ISO/IEC 27036-2 Інформаційні технології. Методи захисту. Інформаційна безпека щодо

взаємовідносин з постачальниками. Частина 2. Загальні вимоги
28. ISO/IEC 27036-3 Інформаційні технології. Методи захисту. Інформаційна безпека щодо взаємовідносин з постачальниками. Частина 3. Настанови щодо безпеки ланцюгів постачання ІКТ
29. ISO/IEC 27037 Інформаційні технології. Методи захисту. Настанови щодо ідентифікації, збирання, отримання та зберігання цифрових доказів
30. ISO/IEC 29100 Інформаційні технології. Методи захисту. Основні положення щодо приватності
31. ISO/IEC 29101 Інформаційні технології. Методи захисту. Основні положення щодо архітектури приватності
32. ISO/IEC 31000 Управління ризиками. Принципи та настанови.
33. ISO/IEC TR 27008 Інформаційні технології. Методи захисту. Настанови для аудиторів заходів інформаційної безпеки
34. ISO/IEC Директиви. Частина 2
35. Андрєєв В.І., Хорошко В.О., Чередніченко В.С., Шелест М.Є., Основи інформаційної безпеки. Підручник. – К.: вид. ДУІКТ, 2009. –292 с.
36. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с.
37. 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.
38. Кобозева А.А., Мачалін І.О., Хорошко В.О., Аналіз захищеності інформаційних систем. Підручник. – К.: вид. ДУІКТ, 2010. - 316 с.
39. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
40. Цимбалюк В.С. Інформаційне право (теорія і практика). Монографія. – К.: 2009. - 364 с.

Допоміжна

1. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін.]. – К. : Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.
2. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.
3. 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.
4. 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.
5. Єрмошин В.В., Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки. /Невойт Я.В., Єрмошин В.В.// Монографія. – К: ДУТ, 2015. – 124 С.
6. Кримінально-правова охорона інформаційної безпеки України: монограф. / М.В. Карчевський ; МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. – 528 с.
7. Прикладні аспекти аналізу та синтезу політик безпеки : навч. посіб. / В.А. Козачок, Н.В. Коршун, Н.П. Мазур, А.В. Платоненко, П.М. Складанний – К.: Київський університет імені Бориса Грінченка, 2021. – 267 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/.
4. 101 Free Admin Tools [Електронний ресурс]. – Режим доступу: https://techtalk.gfi.com/101-free-admin-tools/