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
«___» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА СУЧАСНОГО ПІДПРИЄМСТВА»

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 № 3338/23
(підпис) (прізвище, ініціали)
«___» 2023 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	4 / 120	
Курс	4	
Семестр	8	
Кількість змістових модулів з розподілом:	2	
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 «Інформаційна та кібербезпека сучасного підприємства» 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 «Інформаційна та кібербезпека сучасного підприємства» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Інформаційна та кібербезпека сучасного підприємства» складається з двох змістовних модулів. Обсяг дисципліни – 120 год. (4 кредити).

Метою викладання навчальної дисципліни «Інформаційна та кібербезпека сучасного підприємства» є формування у студентів уміння вирішувати задачі створення та аналізу різноманітних типових технологій побудови систем інформаційної та кібернетичної безпеки сучасного підприємства та захисту цінних інформаційних ресурсів, застосовувати нормативно-правові, організаційні та технічні процедури підчас побудови та експлуатації систем управління інформаційною безпекою на підприємстві.

Завдання полягає у формуванні теоретичних знань та практичних умінь у сфері кіберзахисту підприємства 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.

КФ 8 – Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 12 – Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та

дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

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 висуваються ними при побудові захищених систем, особливості підтвердження відповідності побудованих систем захисту; принципи побудови систем захисту інформації і кіберзахисту; основні методи, засоби і технології що призначені для забезпечення інформаційної безпеки та кібербезпеки.

вміти:

- розробляти та визначати принципи побудови систем інформаційної та кібернетичної безпеки сучасного підприємства;
- здійснювати обстеження об'єктів інформаційної діяльності, формувати вихідні дані для проектування системи захисту та визначати склад потрібного апаратного та програмного засобів захисту;
- здійснити формування моделі загроз та моделі порушника інформаційної безпеки, базових положень політики безпеки, розробляти правила забезпечення інформаційної та кібербезпеки;
- здійснювати аудит та оцінку ефективності функціювання систем захисту інформації та систем управління інформаційною безпекою сучасного підприємства;
- застосувати національні та міжнародні стандарти для аналізу та розробки систем інформаційної та кібернетичної безпеки сучасного підприємства та її складових,

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

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

ПРз-8 — вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; проводити розслідування інцидентів інформаційної безпеки та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної безпеки та/або кібербезпеки; забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації.

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. Інформаційна та кібербезпека сучасного підприємства							
Тема 1. Складові інформаційної безпеки та кібербезпеки сучасного підприємства	22	4	4	4			10
Тема 2. Формування вихідних даних до проекту системи ІБ	24	4	6	4			10
Модульний контроль	4						
Разом	50	8	10	8			20
Змістовий модуль 2. Методи, засоби та технології захисту інформації та кіберзахисту сучасного підприємства							
Тема 3: Складові системи ІБ та кібербезпеки підприємства, огляд технологій захисту	26	6	2	4			14
Тема 4. Процесний підхід до побудови системи управління ІБ на підприємстві	22	4	2	4			12
Тема 5: Форми і методи аудиту інформаційної безпеки на підприємстві	18	2	4	2			10
Модульний контроль	4						
Разом	70	12	8	10			36
Усього	**120**	**20**	**18**	**18**			**56**

5. Програма навчальної дисципліни

Змістовий модуль 1. Нормативні основи забезпечення інформаційної та кібернетичної безпеки сучасного підприємства

Тема 1. Складові інформаційної безпеки та кібербезпеки сучасного підприємства

Лекція 1. Сучасне підприємство: бізнес процеси, ІТ, інформаційна та кібернетична безпека.

Поняття про бізнес-процеси сучасного підприємства. Інформаційні технології на підприємстві. Базові складові інформаційної безпеки. Правові аспекти інформаційної безпеки та кібербезпеки. Основні поняття інформаційної безпеки та кібербезпеки підприємства. Характеристика інформації на підприємстві та цілі її захисту.

Лекція 2. Політика інформаційної безпеки підприємства

Політика інформаційної безпеки (ІБ): цілі, завдання, зміст. Принципи формування політики безпеки підприємства. Часткові політики безпеки.

Тема 2. Формування вихідних даних до проекту системи ІБ

Лекція 3. Передпроектний етап: побудова моделі загроз ІБ і моделі порушника

Мета та завдання перед проектного етапу: підготовка вихідних даних та обстеження об’єкту інформаційної діяльності. Класифікація та оцінка інформаційних ресурсів. Задачі моделювання. Формування моделі загроз ІБ на підприємстві. Побудова моделі порушника ІБ.

Лекція 4. Процедури управління ризиками ІБ

Умови забезпечення ІБ на підприємстві та можливі ризики. Поняття про управління ризиками ІБ. Обробка ризиків. Методики аналізу та оцінки ризиків.

Змістовий модуль 2. Методи, засоби та технології захисту інформації та кіберзахисту сучасного підприємства

Тема 3. Складові системи ІБ та кібербезпеки підприємства, огляд технологій захисту

Лекція 5. Технічний захист інформації на підприємстві

Комплексний підхід до забезпечення ІБ. Канали впливу/ витоку інформації на підприємстві: електричні, електромагнітні, акустичні, оптичні, несанкціонованого доступу (НСД) в комп'ютерних системах. Нормативні вимоги щодо технічного захисту інформації (ЗІ). Методи ЗІ від впливу/ витоку за рахунок технічних каналів. Спеціальні дослідження технічних засобів.

Лекція 6. Технології криптографічного захисту інформації на підприємстві

Характеристика засобів криптографічного захисту. Вимоги до сучасних криптосистем. Технології шифрування та цифрового підпису на підприємстві. Забезпечення безпеки криптографічних ключів. Сутність та застосування криптопротоколів. Основи застосування технології блокчейн.

Лекція 7. Сучасні методи забезпечення комп'ютерної безпеки

Критерії захищеності комп'ютерних систем. Сегментація мереж. Еталонна модель системи захисту та її складові: розмежування доступу, антивірусний захист, криптографічний захист, захист від DDoS атак, технології IDS/ IPS, захист серверів і баз даних. Обробка інформації про кіберінциденти SIEM. Резервне копіювання та відновлення інформації. Безпека хмарних інформаційних технологій.

Тема 4. Процесний підхід до побудови системи управління інформаційною безпекою (СУІБ)

Лекції 8. Процесний підхід до побудови СУІБ

Нормативні вимоги щодо СУІБ. Переваги впровадження СУІБ. Формування Політики ІБ та побудова СУІБ. Сертифікація СУІБ на відповідність вимогам стандарту ISO/IEC 27001.

Лекції 9. Управління інцидентами інформаційної безпеки

Управління інцидентами інформаційної безпеки. Процедури відновлення ІТ-інфраструктури після кіберінцидентів.

Тема 5. Форми і методи аудиту інформаційної безпеки на підприємстві

Лекція 10. Методика аудиту безпеки інформаційної інфраструктури підприємства

Аудит інформаційної безпеки (ІБ) на підприємстві: об'єкти, суб'єкти і види аудита Базові підходи до проведення аудиту ІБ, вимоги до аудиторів. Методичні аспекти внутрішнього аудиту ІБ. Організація зовнішнього аудиту ІБ. Основні заходи службового розслідування кіберінцидентів.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної звітності, обов'язковості 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.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, залік.
- *Комп'ютерного контролю:* програми – емулятори, віртуальні машини.
- *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	4	4	6	6
Відвідування семінарських занять	1	5	5	4	4
Відвідування практичних занять	1	4	4	5	5
Робота на семінарському занятті	10	5	50	4	40
Робота на практичному занятті	10	4	40	5	50
Виконання завдань для самостійної роботи	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25
Разом		-	133	-	135
Максимальна кількість балів:		268			
Розрахунок коефіцієнта:		268/100=2,68			

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. Нормативні основи забезпечення інформаційної та кібернетичної безпеки сучасного підприємства			
1	Складові інформаційної безпеки та кібербезпеки сучасного підприємства. Формування вихідних даних проекту системи ІБ: • виконання завдань відповідно до теми; • опрацювання фахових видань.	24	5
Змістовий модуль 2. Методи, засоби та технології захисту інформації та кіберзахисту сучасного підприємства			
2	Складові системи ІБ та кібербезпеки підприємства, огляд технологій захисту. Процесний підхід до побудови системи управління інформаційною безпекою. Форми і методи аудиту інформаційної безпеки на підприємстві: • виконання завдань відповідно до теми;	40	5

№ з/п	Назва теми	Кількість годин	Бали
	• опрацювання фахових видань.		
	Разом	64	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 допуску до якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Орієнтовний перелік питань для самоконтролю

1. Поняття про бізнес-процеси сучасного підприємства
2. Інформаційні технології на підприємстві
3. Складові інформаційної безпеки
4. Правові аспекти інформаційної безпеки та кібербезпеки
5. Основні поняття інформаційної безпеки та кібербезпеки підприємства
6. Характеристика інформації на підприємстві
7. Цілі та завдання захисту інформації
8. Цілі розробки Політики інформаційної безпеки (ПІБ), її завдання та зміст.
9. Принципи формування ПІБ
10. Часткові політики безпеки
11. Мета та завдання перед проектного етапу: підготовка вихідних даних та обстеження об'єкту інформаційної діяльності.
12. Класифікація та оцінка інформаційних ресурсів.
13. Задачі моделювання.
14. Формування моделі загроз ІБ на підприємстві.
15. Побудова моделі порушника ІБ.
16. Умови забезпечення ІБ на підприємстві та можливі ризики.
17. Поняття про управління ризиками ІБ.
18. Обробка ризиків.
19. Методики аналізу та оцінки ризиків.
20. Комплексний підхід до забезпечення ІБ.
21. Канали впливу/ витоку інформації на підприємстві.
22. Нормативні вимоги щодо технічного захисту інформації (ЗІ).
23. Методи ЗІ від впливу/ витоку за рахунок технічних каналів.
24. Спеціальні дослідження технічних засобів.
25. Характеристика засобів криптографічного захисту.

26. Вимоги до сучасних криптосистем.
27. Технології шифрування та цифрового підпису на підприємстві.
28. Забезпечення безпеки криптографічних ключів.
29. Сутність та застосування криптопротоколів.
30. Основи застосування технології блокчейн.
31. Нормативні вимоги щодо СУІБ.
32. Переваги впровадження СУІБ.
33. Формування Політики ІБ та побудова СУІБ.
34. Сертифікація СУІБ на відповідність вимогам стандарту ISO/IEC 27001.
35. Управління інцидентами інформаційної безпеки.
36. Процедури відновлення ІТ-інфраструктури після кіберінцидентів.
37. Аудит інформаційної безпеки (ІБ) на підприємстві: об'єкти, суб'єкти і види аудита.
38. Базові підходи до проведення аудиту ІБ, вимоги до аудиторів.
39. Методичні аспекти внутрішнього аудиту ІБ.
40. Організація зовнішнього аудиту ІБ.

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 – 20 год., семінарські заняття – 18 год., практичні заняття – 18 год., самостійна робота – 64 год.

Модулі (назви, бали)	**Змістовий модуль 1. Інформаційна та кібербезпека сучасного підприємства (133 бали)**				**Змістовий модуль 2. Методи, засоби та технології захисту інформації та кіберзахисту сучасного підприємства (135 балів)**					
Лекції (теми, бали)	Сучасне підприємство: бізнес процеси, ІТ, інформаційна та кібернетична безпека. (1 бал)	Політика інформаційної безпеки підприємства (1 бал)	Передпроектний етап: побудова моделі загроз ІБ і моделі порушника (1 бал)	Процедури аналізу та оцінки ризиків ІБ (1 бал)	Технічний захист інформації на підприємстві (1 бал)	Технології КЗІ на підприємстві (1 бал)	Методи забезпечення комп'ютерної безпеки (1 бал)	Процесний підхід до побудови СУІБ (1 бал)	Управління інцидентами інформаційної безпеки (1 бал)	Методика аудиту безпеки інформаційної інфраструктури підприємства (1 бал)
Семінарські заняття (теми, бали)	Сучасне підприємство: бізнес процеси, ІТ, інформаційна та кібернетична безпека (11 балів)	Політика інформаційної безпеки підприємства (11 балів)	Передпроектний етап: побудова моделі загроз ІБ і моделі порушника (11 балів)	Процедури аналізу та оцінки ризиків ІБ (22 бали)	Технічний захист інформації на підприємстві (11 балів)	Технології КЗІ на підприємстві (11 балів)		Процесний підхід до побудови СУІБ (11 балів)	Управління інцидентами інформаційної безпеки (11 балів)	
Практичні заняття (теми, бали)	Сучасне підприємство: бізнес процеси, ІТ, інформаційна та кібернетична безпека (11 балів)	Політика інформаційної безпеки підприємства (11 балів)	Передпроектний етап: побудова моделі загроз ІБ і моделі порушника (11 балів)	Процедури аналізу та оцінки ризиків ІБ (11 балів)	Технічний захист інформації на підприємстві (11 балів)	Технології КЗІ на підприємстві (11 балів)	Методи забезпечення комп'ютерної безпеки (11 балів))	Процесний підхід до побудови СУІБ (11 балів)		Методика аудиту безпеки інформаційної інфраструктури підприємства (11 балів)
Поточний контроль (вид, бали)	Модульна контрольна робота №1 (25 балів)				Модульна контрольна робота №2 (25 балів)					
Самостійна робота	Самостійна робота 1 (5 балів)				Самостійна робота 2 (5 балів)					
Підсумковий контроль (вид, бали)	Залік									

8. Рекомендовані джерела

Основна (базова):

1. 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).
2. Lakhno, V., Husiev, B., Smolii, V., Blozva, A., Kasatkin, D., & Osypova, T. (2021). Методи системного аналізу при формуванні політики інформаційної безпеки на транспорті. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(12), 51-60. https://doi.org/10.28925/2663-4023.2021.12.5160.
3. Skiter, I. (2021). Модель оцінки рівня культури кібербезпеки в інформаційній системі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(13), 158-169. https://doi.org/10.28925/2663-4023.2021.13.158169.
4. Smirnova, T., Polishchuk , L., Smirnov, O., Buravchenko, K., & Makevnin, A. (2020). Дослідження хмарних технологій як сервісів. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 3(7), 43-62. https://doi.org/10.28925/2663-4023.2020.7.4362
5. Tsyrkaniuk, D., Sokolov, V., Mazur, N., Kozachok, V., & Astapenya, V. (2021). Метод побудови профілів користувача маркетплейсу і зловмисника. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(14), 50-67. https://doi.org/10.28925/2663-4023.2021.14.5067.
6. Yakymenko, Y., Muzhanova, T., & Lehominova, S. (2021). Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії FIREEYE. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(12), 36-50. https://doi.org/10.28925/2663-4023.2021.12.3650.
7. Г.М. Гулак, О.Б. Жильцов, П.М. Складанний, Р.В. Киричок, Н.В. Коршун Інформаційна та кібернетична безпека підприємства / Навчальний підручник. КУБГ. – К. 2022. 451с.
8. Гулак Г. М., Скітер І. С., Гулак Є. Г. Методологічні засади створення та функціонування центру кібербезпеки інформаційної інфраструктури об'єктів ядерної енергетики. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка". 2021. Т. 4, № 12. С. 172–186. DOI: https://doi.org/10.28925/2663-4023.2021.12.172186.
9. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с.
10. ДСТУ ISO 19011:2012 Настанови щодо здійснення аудитів систем управління (ISO 19011:2011, IDT).
11. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).
12. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT).
13. НД ТЗІ 1.1-003-99, «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу», - 30с.
14. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

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., Юдін О.К., Інформаційна безпека держави. –К.: «МК-Прес», 2005. – 432с.
5. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 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. 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 assurance 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. Switzerland, 1989. 32 pp.
12. 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.

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/.