

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

Навчально-науковий інститут автоматики та електротехніки
Кафедра комп'ютерних технологій та інформаційної безпеки

Код за ОПІ
ПП12

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної
роботи, к.т.н., доцент
С.О. Слободян
_____ 2023 р.



РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Program of the Discipline

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ
Information security management

Рівень вищої освіти _____ перший (бакалаврський)
Тип дисципліни _____ обов'язкова
Мова викладання _____ українська

Миколаїв 2023 рік

Робоча програма навчальної дисципліни «Управління інформаційною безпекою» є однією із складових комплексної підготовки фахівців галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека та захист інформації», освітня програма «Системи технічного захисту інформації, автоматизація її обробки»

«__» _____ 2023 р. – 36 с.

Розробник: Турти М.В., доцент кафедри Комп'ютерних технологій та інформаційної безпеки, канд. техн. наук, доцент

Проект робочої програми навчальної дисципліни «Управління інформаційною безпекою» узгоджено з гарантом освітньої програми

Гарант освітньої програми «Системи технічного захисту інформації, автоматизація її обробки»

Нужний С.М., канд. техн. наук, доцент



Проект робочої програми навчальної дисципліни «Управління інформаційною безпекою» розглянуто на засіданні кафедри КТІБ.

Протокол від «13» 06 2023 р. № 12.

Завідувач кафедри КТІБ, к.т.н., доцент

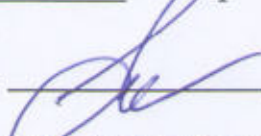


С.М. Нужний

Проект робочої програми навчальної дисципліни «Управління інформаційною безпекою» розглянуто методичною радою Навчально-наукового інституту автоматики та електротехніки.

Протокол від «30» 08 2023 р. № 1.

Голова, к.т.н., доц.



Д.О.Жук

Проект робочої програми навчальної дисципліни «Управління інформаційною безпекою» погоджено з навчальним відділом.

Начальник навчального відділу, к.т.н., доцент



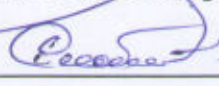
А.В. Лабарткава

Робочу програму навчальної дисципліни «Управління інформаційною безпекою» затверджено Навчально-методичною радою НУК ім. адм. Макарова.

Протокол від «7» 09 2023 р. № 6.

Голова Навчально-методичної ради НУК ім. адм. Макарова,

д.т.н., професор



Є.І. Трушляков

ЗМІСТ

Вступ.....	4
1. Опис навчальної дисципліни	5
2. Мета навчальної дисципліни	6
3. Передумови для вивчення навчальної дисципліни	7
4. Очікувані результати навчання	7
5. Програма навчальної дисципліни	8
6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування.....	18
7. Форми поточного та підсумкового контролю	19
8. Критерії оцінювання результатів навчання.....	21
9. Засоби навчання	26
10. Рекомендовані джерела інформації.....	27

ВСТУП

Анотація

Навчальна дисципліна «Управління інформаційною безпекою» є дисципліною професійної підготовки бакалаврів зі спеціальності 125 «Кібербезпека та захист інформації». Дана дисципліна є обов'язковим компонентом освітньої програми, який забезпечує теоретичну та практичну підготовку студентів до вирішення адміністративно – правових питань захисту інформації, оцінювання ризиків інформаційної безпеки і якості комплексних систем захисту інформації. Отримані слухачами курсу теоретичні знання та практичні навички є базовим програмним результатом навчання та формують фахову компетентність.

Ключові слова: інформаційна безпека, системи управління інформаційною безпекою, нормативно-правова база захисту інформації, ризики інформаційної безпеки, методи оцінювання ризиків, критерії оцінювання якості комплексних систем захисту інформації

Abstract

The educational discipline "Information security management" is a discipline of professional training of bachelors in the specialty 125 "Cybersecurity and information protection ". This discipline is a mandatory component of the educational program, which provides theoretical and practical training of students to solve administrative and legal issues of information protection, assessment of information security risks and the quality of comprehensive information security systems. The theoretical knowledge and practical skills acquired by the students of the course are the basic program outcome of the study and form professional competence.

Keywords: information security, information security management systems, information protection regulatory framework, information security risks, risk assessment methods, criteria for evaluating the quality of comprehensive information security systems

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 9	Галузь знань 12 Інформаційні технології Спеціальність: 125 Кібербезпека та захист інформації	Обов’язкова	
Модулів – 3	Освітня програма «Системи технічного захисту інформації, автоматизація її обробки»	Рік підготовки	
Змістових модулів – 4		2-й, 3-й	2-й, 3-й
Курсова робота “Оцінювання ефективності систем захисту інформації”		Семестр	
Загальна кількість годин – 270		4-й, 5-й	4-й, 5-й
		Індивідуальне науково-дослідне завдання – курсова робота	
Тижневих годин для денної форми навчання: 4-й семестр: Аудиторних – 2; Самостійної роботи: – 4. 5-й семестр: Аудиторних – 3; Самостійної роботи: – 9.	Рівень вищої освіти: перший (бакалаврський)	Лекції, год	
		30 год.	8 год.
		Лабораторні роботи, год.	
		45 год.	8 год.
		Практичні роботи, год.	
		-	-
		Самостійна робота, год.	
		195	254
	Вид контролю: 4-й семестр – екзамен 5-й семестр - курсова робота, екзамен		
	Форма контролю: усна, письмова		

2. Мета навчальної дисципліни

Метою вивчення навчальної дисципліни «Управління інформаційною безпекою» є формування у майбутніх фахівців відповідного рівня підготовки з питань застосування нормативно-правових актів і методів оцінювання якості захисту інформації в автоматизованих системах.

Завданнями дисципліни є теоретична та практична підготовка студентів для вирішення конкретних фахових питань, таких як: нормативно-правове обґрунтування проектних рішень в галузі захисту інформації в автоматизованих системах, організація діяльності служби захисту інформації, визначення та оцінювання показників рівня безпеки об'єктів інформаційної діяльності, управління процесом забезпечення інформаційної безпеки із застосуванням аналізу організаційно-правових, технічних, криптографічних та оперативно-розшукових заходів у цій сфері для формування наступних компетентностей.

- (ЗК1) - Здатність застосовувати знання у практичних ситуаціях;
- (ФК1) - 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;
- (ФК2) - Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки;
- (ФК3) - Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах;
- (ФК8) - Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку;
- (ФК9) - Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою;
- (ФК12) - 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. Передумови для вивчення навчальної дисципліни

Для ефективного вивчення дисципліни «Управління інформаційною безпекою», студенти повинні засвоїти матеріал з дисципліни:

- Інформаційні технології систем управління та захисту інформації;
- Базы даних;
- Системи і мережі передачі даних.

4. Очікувані результати навчання

Основними (програмними) результатами навчання з дисципліни «Управління інформаційною безпекою» є:

- (РН 5) Адаптуватися в умовах частотої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
- (РН 7) - Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
- (РН8) - Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
- (РН9) - Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
- (РН13) аналізувати проекти інформаційно-комунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
- (РН15) використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
- (РН21) вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-комунікаційних (автоматизованих) системах;
- (РН22) вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки;

- (PH24) вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
- (PH25) забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в' інформаційних та інформаційно-комунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;
- (PH26) впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-комунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
- (PH32) Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
- (PH33) - Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
- (PH34) - Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
- (PH41) – Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
- (PH42) - Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
- (PH43) - Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів;
- (PH44) - Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;

5. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. Основи управління інформаційною безпекою в Україні

Тема 1. Інформація як предмет захисту. [1] – с.9-15, 18; [2] – с.9-13, 112-116; [3] – с.5-7; [4] – с.6-7; [43]; [44].

Тема 2. Представлення інформації. [6] – с.56-77.

Тема 3. Демаскуючі ознаки об'єктів захисту. [7] - с.2-43.

Тема 4. Види загроз безпеці інформації. Принципи і технології добування інформації. [1] – с.27-75, 77-100, 145, 163-166, 173-175, 180, 184-187; [2] – с.117-127; [3] – с.25-52; [4] – с.7-20; [5] – с.6-33, 68-74.

Змістовий модуль 2. Організаційні засади управління інформаційною безпекою

Тема 5. Державне регулювання захисту інформації в Україні [1] – с.74-77, ; [5] – с.125-137; [9]; [11]; [12]; [13]; [14]; [18]; [19]; [20]; [21].

Тема 6. Нормативно-правова база захисту інформації [1] – с.18-27, [2] – с.164-189; [3] – с.7-19; [4] – с.44-52; [5] – с.35-67; [8] – с.7-40

Тема 7. Система управління інформаційною безпекою [1] – с.183, 196-207; [8] – с.91-196; [21]

Тема 8. Ризики інформаційної безпеки [2] с.131-135; [5] – с.102-111; [8] – с.73-89.

Модуль 2

Змістовий модуль 3. Нормативні вимоги до діяльності в галузі кібербезпеки

Тема 9. Міжнародні і національні нормативні документи в галузі кібербезпеки [5] – с.61-67, 109; [8] – с.7-40; [22-42].

Тема 10. Стандартні функціональні профілі захищеності [2] – с.172-177; [46], [47]; [51-55]

Тема 11. Ліцензування та сертифікація в галузі інформаційної безпеки [15]

Тема 12. Вимоги до захисту інформації на Web-сторінках і АС2. [48], [49]

Змістовий модуль 4. Розв’язок прикладних задач управління інформаційною безпекою

Тема 13. Організація служби захисту інформації організації [2] – с.192-199; [4] – с.21-28, 40-44; [5] – с.121-124; [8] – с.41-72; [21]; [45]

Тема 14. Галузеві особливості управління інформаційною безпекою [10]; [16]; [17]; [58]; [61-64]

Тема 15. Формування вимог до СУІБ і оцінювання її ефективності [1] – с.115-118, 183-195; [2] – с.131-138; [5] – с.102-110; [8] – с.73-89; [22-42]; [46]; [47]; [50]; [56-59].

Модуль 3

Індивідуальне науково-дослідне завдання (ІНДЗ):
курсова робота на тему " Оцінювання ефективності систем захисту інформації
" _____ ".
(назва об'єкта інформаційної діяльності)

Тематичний план навчальної дисципліни

Назви змістових модулів і тем	Кількість годин							
	денна форма				заочна форма			
	усього	у тому числі			усього	у тому числі		
		л	лаб	с.р.		л	лаб	с.р.
Модуль 1 (М1)								
Змістовий модуль 1. Основи управління інформаційною безпекою в Україні								
Тема 1. Інформація як предмет захисту	4	2	-	2	4	2	-	2
Тема 2. Представлення інформації	10	2	2	6	10		-	10
Тема 3. Демаскуючі ознаки об’єктів захисту	6	2	-	4	6		-	6
Тема 4. Види загроз безпеці інформації. Принципи і технології добування інформації.	10	2	2	6	10		2	8
Разом за змістовим модулем 1	30	8	4	18	30	2	2	26
Змістовий модуль 2. Організаційні засади управління інформаційною безпекою								
Тема 5. Державне регулювання захисту інформації в Україні	13	2	4	9	13	2	-	11
Тема 6. Нормативно-правова база захисту інформації	20	2	2	14	20		2	18
Тема 7. Система управління інформаційною безпекою	13	2	2	9	13		-	13
Тема 8. Ризики інформаційної безпеки	14	1	3	10	14		-	14
Разом за змістовим модулем 2	60	7	11	42	60	2	2	56
Разом за модулем 1	90	15	15	60	90	4	4	82
Модуль 2 (М2)								
Змістовий модуль 3. Нормативні вимоги до діяльності в галузі кібербезпеки								
Тема 9. Міжнародні і національні нормативні документи в галузі кібербезпеки	8	2	2	4	8	2	-	6
Тема 10. Стандартні функціональні профілі захищеності	18	2	8	8	18		2	16
Тема 11. Ліцензування та сертифікація в галузі інформаційної безпеки	8	2	2	4	8		-	8

Назви змістових модулів і тем	Кількість годин							
	денна форма				заочна форма			
	усього	у тому числі			усього	у тому числі		
		л	лаб	с.р.		л	лаб	с.р.
Тема 12. Вимоги до захисту інформації на Web-сторінках і АС2	11	2	4	5	11		-	11
Разом за змістовим модулем 3	45	8	16	21	45	2	2	41
Змістовий модуль 4. Розв'язок прикладних задач управління інформаційною безпекою								
Тема 13. Організація служби захисту інформації організації	9	2	2	5	9	2	-	7
Тема 14. Галузеві особливості управління інформаційною безпекою	17	2	6	9	17		-	17
Тема 15. Формування вимог до СУІБ і оцінювання її ефективності	19	3	6	10	19		2	17
Разом за змістовим модулем 4	45	7	14	24	45	2	2	41
Разом за модулем 2	90	15	30	45	90	4	4	82
Модуль 3 (М4)								
Курсовий проект	90	-	-	90	90	-	-	90
Разом (М1+М2+М3)	270	30	45	195	270	8	8	254

Для студентів заочної форми навчання читаються оглядові лекції за темами змістових модулів в обсягах відповідно до вищенаведеної таблиці.

Теми практичних занять

Практичні роботи програмою не передбачені

Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		ДФН	ЗФН
Модуль 1			
Змістовий модуль 1. Основи управління інформаційною безпекою в Україні			
1	Інформація як предмет захисту	2	-
2	Інциденти в галузі інформаційної безпеки	2	2
Разом за змістовим модулем 1		4	2

№ з/п	Назва теми	Кількість годин	
		ДФН	ЗФН
Змістовий модуль 2. Організаційні засади управління інформаційною безпекою			
3	Державна служба спеціального зв'язку та захисту інформації	2	-
4	Державне регулювання в галузі інформаційної безпеки	2	-
5	Нормативно-правова база діяльності в галузі захисту інформації	2	2
6	Політика інформаційної безпеки	2	-
7	Управління ризиками безпеки	2	-
8	Спеціалізоване програмне забезпечення в галузі інформаційної безпеки	1	-
Разом за змістовим модулем 2		11	2
Разом за модулем 1		15	4
Модуль 2			
Змістовий модуль 3. Нормативні вимоги до діяльності в галузі кібербезпеки			
9	Міжнародні та вітчизняні стандарти в галузі управління, оцінки та аудиту інформаційної безпеки	2	-
10	Критерії оцінювання захищеності інформації від несанкціонованого доступу	2	2
11	Стандартні функціональні профілі захищеності	2	-
12	Розробка методики перевірки відповідності функціональних послуг безпеки	2	-
13	Перевірка відповідності профілю захищеності міжнародним стандартам	2	-
14	Ліцензування та сертифікація в галузі інформаційної безпеки Регіональні ліцензіати в галузі інформаційної безпеки	2	-
15	Вимоги до захисту інформації на Web-сторінках	2	-
16	Захист інформації в автоматизованих системах другого класу	2	-
Разом за змістовим модулем 3		16	2
Змістовий модуль 4. Розв'язок прикладних задач управління інформаційною безпекою			
17	Служба захисту інформації	2	
18	Управління інформаційною безпекою в банківських установах	2	

№ з/п	Назва теми	Кількість годин	
		ДФН	ЗФН
19	Управління інформаційною безпекою на об'єктах критичної інфраструктури	2	-
20	Управління інформаційною безпекою в морській галузі	2	-
21	Оцінювання ризиків інформаційної безпеки	2	2
22	Управління ризиками інформаційної безпеки	2	-
23	Формування вимог до СУІБ	2	-
Разом за змістовим модулем 4		14	2
Разом за модулем 2		30	4
Разом (М1+М2)		45	8

Студенти заочної форми виконують лабораторні роботи № 2, 5, 10, 21.

Самостійна робота

Самостійна робота здобувача вищої освіти є однією з форм організації навчання, основною формою оволодіння навчального матеріалу в час, вільний від обов'язкових навчальних занять.

Метою самостійної роботи є повторення й осмислення студентом основних питань кожної теми, висвітлених на лекційних і лабораторних заняттях. Самостійна робота проводиться в лабораторіях НУК, читальних залах, на об'єктах майбутньої діяльності і/або вдома. Результати цієї роботи фіксуються студентом в індивідуальному робочому зошиті (конспекті).

Навчальний матеріал дисципліни, передбачений для засвоєння здобувачем вищої освіти в процесі самостійної роботи, виноситься на підсумковий контроль поряд з навчальним матеріалом, який опрацьовувався при проведенні навчальних занять.

В рамках самостійної роботи також виконується індивідуальне науково-дослідне завдання у формі курсової роботи.

Розподіл годин самостійної роботи для денної форми навчання:

- підготовка до лекційних занять – 0,5 год. / 1 заняття (на 1 лекцію);
- самостійне опрацювання окремих тем навчальної дисципліни (які не викладаються на лекціях) – 0,25-2 год. / 1 заняття;
- підготовка до лабораторних занять – 1-2 год. / 1 заняття;
- підготовка до модульних контрольних робіт 4-5 год на 1 роботу
- підготовка до екзаменів – 15 год. на 1 захід.

Розподіл годин самостійної роботи для заочної форми навчання:

- підготовка до лекційних занять – 0,5 - 2 год. / 1 заняття (на 1 лекцію);
- самостійне опрацювання окремих тем навчальної дисципліни (які не викладаються на лекціях) – 1-3 год. / 1 заняття;
- підготовка до лабораторних занять – 5 год. / 1 заняття;
- підготовка до модульних контрольних робіт 15 год на 1 роботу
- підготовка до екзаменів – 29 год. на 1 захід.

Розподіл годин самостійного опрацювання окремих тем навчальної дисципліни

№ з/п	Назва теми	Кількість годин	
		Д.Ф.Н	З.Ф.Н.
М1			
1	До теми 1. Захист інформації в data center	1	1
2	До теми 2. RAID-масиви	2	2
3	До теми 3. Принципи виявлення рухомих об'єктів за відеореєстром	2	2
4	До теми 4. Загрози інформаційній безпеці IoT	2	2
5	До теми 5. Історія ДССЗІ	1	1
6	До теми 6. Нормування захисту інформації в морській галузі	2	2
7	До теми 7. Інциденти інформаційної безпеки за поточний рік	1	1
8	До теми 8. Сучасна статистика збитків від порушення інформаційної безпеки в світі	1	1
Усього годин за модуль 1		12	12
М2			
9	До теми 9. Нормативні документи Євросоюзу в галузі кібербезпеки	0,5	2
10	До теми 10. Етапи створення КСЗІ	0,25	1
11	До теми 11. Регіональні ліцензіати в галузі інформаційної безпеки	0,25	1
12	До теми 12. Статистика сучасних атак на Web-ресурси	0,25	1
13	До теми 13. Кіберполіція: задачі, організація, кадрові вимоги	0,25	2
14	До теми 14. Організація захисту інформації в авіації	0,5	2
15	До теми 15. Методи оцінювання доцільності інвестицій в кібербезпеку	1,0	3
Усього годин за модуль 2		3	12
Разом		15	24

Розподіл годин підготовки самостійної роботи

№	Вид роботи	Кількість годин	
		Денна форма навчання	Заочна форма навчання
М1			
1	Підготовка до лекцій	8	1
2	Підготовка до лабораторних робіт	15	10
3	Підготовка до модульних контрольних робіт	10	30
4	Самостійне опрацювання окремих тем навчальної дисципліни	12	12
5	Підготовка до екзамену	15	29
Усього годин за модуль 1		60	82
М2			
1	Підготовка до лекцій	4	1
2	Підготовка до лабораторних робіт	15	10
3	Підготовка до модульних контрольних робіт	8	30
4	Самостійне опрацювання окремих тем навчальної дисципліни	3	12
5	Підготовка до екзамену	15	29
Усього годин за модуль 2		45	82
М3			
1	Курсова робота	90	90
Усього годин за модуль 3		90	90
Разом за курсом		195	254

Індивідуальне науково-дослідне завдання

Індивідуальне навчально-дослідне завдання (ІНДЗ) виконується здобувачем під керівництвом викладача і полягає у виконанні курсової роботи у п'ятому семестрі.

Індивідуальні завдання на курсову роботу видаються студентам на другому тижні п'ятого семестру.

Виконання курсової роботи створює умови для якнайповнішої реалізації творчих можливостей студентів і має на меті поглиблення, узагальнення та закріплення знань, які здобувачі одержують у процесі навчання, а також застосування знань на практиці.

Індивідуальні завдання виконуються самостійно і не входять до тижневого аудиторного навантаження здобувача. Викладач контролює

виконання індивідуального завдання на консультаціях. Студент несе особисту відповідальність за прийняті в роботі рішення і правильність виконання і оформлення роботи.

Курсова робота складається з розрахунково-пояснювальної записки та графічної частини (остання - на аркушах формату А3 або А4). Тематика та зміст курсової роботи спрямовані на здобуття студентами практичних навичок опрацювання нормативно-правової бази в галузі інформаційної безпеки та розрахунку показників якості систем захисту. Основою для курсової роботи є лекційний матеріал, нормативно-правова база захисту інформації, поточний стан якої визначається сайтом Державної служби спеціального зв'язку та захисту інформації, а також будівельні креслення об'єкта інформаційної діяльності (за необхідністю), характеристика інформації, що циркулює в системі.

Індивідуальне завдання курсової роботи може бути пов'язане з тематикою наукової діяльності студента.

Метою курсової роботи є визначення ефективності системи захисту інформації для заданого об'єкта інформаційної діяльності.

Робота полягає у формуванні опису об'єкта інформаційної діяльності; визначенні нормативно-правової бази розробки; визначенні стандартного функціонального профілю захищеності, визначення функцій та послуг безпеки, які повинен забезпечувати комплекс засобів захисту, розробці порядку і методики його випробувань, визначення відповідності вимог щодо функціональних послуг безпеки і коректності їх реалізації міжнародним нормативним актам в галузі інформаційної і кібербезпеки, обґрунтованому виборі показників якості системи захисту інформації і системи управління інформаційною безпекою, кількісній оцінці показників якості

До складу курсової роботи входять зміст, вступ, основна частина, висновки, перелік посилань та графічна частина (в разі необхідності), оформлені згідно з вимогами ЄСКД й іншими нормативними документами і виконані студентом у відповідності до індивідуального завдання.

В курсовій роботі мають бути продемонстровані системний підхід до розв'язку задачі та відповідність знань та вмінь студента з дисципліни “Управління інформаційною безпекою” вимогам даної робочої програми.

Тематика курсових робіт:

1. Оцінювання ефективності системи захисту інформаційних ресурсів кафедри.

2. Оцінювання ефективності системи захисту локальної мережі інституту.

3. Оцінювання ефективності системи захисту локальної мережі університету.

4. Оцінювання ефективності системи захисту локальної мережі фірми, що має ліцензію на надання послуг в галузі інформаційної безпеки.

5. Оцінювання ефективності системи захисту локальної мережі медичної установи.

6. Оцінювання ефективності системи захисту локальної мережі районного суду.
7. Оцінювання ефективності системи захисту локальної мережі судноплавної компанії.
8. Оцінювання ефективності системи захисту локальної мережі порту.
9. Оцінювання ефективності системи захисту телекомунікаційної системи судна.
10. Оцінювання ефективності системи захисту кампусної мережі.
11. Оцінювання ефективності системи захисту IP-телефонії кафедри.
12. Оцінювання ефективності системи захисту IP-телефонії інституту.
13. Оцінювання ефективності системи захисту IP-телефонії університету.
14. Оцінювання ефективності системи захисту IP-телефонії фірми, що має ліцензію на надання послуг в галузі інформаційної безпеки.
15. Оцінювання ефективності системи захисту IP-телефонії медичної установи.
16. Оцінювання ефективності системи захисту IP-телефонії районного суду.
17. Оцінювання ефективності системи захисту IP-телефонії судноплавної компанії.
18. Оцінювання ефективності системи захисту IP-телефонії порту.
19. Оцінювання ефективності системи захисту телекомунікаційної системи судна.
20. Оцінювання ефективності системи захисту пристрою мобільного зв'язку.
21. Оцінювання ефективності системи захисту інформаційних ресурсів кафедри.
22. Оцінювання ефективності системи захисту сайту кафедри.
23. Оцінювання ефективності системи захисту сайту університету
24. Оцінювання ефективності системи захисту сайту облдержадміністрації.
25. Оцінювання ефективності системи захисту інтернет-магазину.
26. Оцінювання ефективності системи захисту сайту бібліотеки ім.Вернадського.
27. Оцінювання ефективності системи захисту автоматизованого документообігу вузу.
28. Оцінювання ефективності системи управління інформаційною безпекою на математичних моделях.
29. Оцінювання ефективності системи захисту об'єкта інформаційної діяльності на математичних моделях.
30. Обґрунтування необхідності модернізації системи захисту об'єкта інформаційної діяльності.

6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування

Здобувач зобов'язаний вивчити теоретичний матеріал та здобути практичні навички у відповідності до тематичного плану навчальної дисципліни.

Методами навчання є:

- пояснення, демонстрування;
- лекція; відеометод;
- робота з літературою;
- лабораторна робота;
- інструктаж (інструктаж з техніки безпеки та пожежної безпеки проводиться одноразово на першому занятті в лабораторії);
- репродуктивний метод;
- проблемного викладу.

При вивченні дисципліни використовуються 3 групи методів навчання:

I група методів - методи організації та здійснення навчально-пізнавальної діяльності:

- словесні: розповідь-пояснення, лекція;
- наочні: ілюстрація, презентація, демонстрація;
- практичні: лабораторні роботи;
- індуктивні методи: узагальнення, пов'язані із проведенням експериментів;
- дедуктивні методи: розвиток абстрактного мислення для засвоєння навчального матеріалу на основі узагальнень;
- репродуктивні методи: робота за готовими прикладами;
- творчі, проблемно-пошукові методи: самостійна, творча пізнавальна діяльність;
- навчальна робота студентів під керівництвом НПП;
- самостійна робота студентів.

II група методів - методи стимулювання й мотивації навчально-пізнавальної діяльності:

- методи стимулювання інтересу до навчання: створення ситуації інтересу при викладанні матеріалу; аналіз життєвих ситуацій;
- методи стимулювання обов'язку й відповідальності: роз'яснення мети навчального предмета; вимоги до вивчення предмета; заохочення та покарання в навчанні;

III група методів - методи контролю (самоконтролю, взаємоконтролю), корекції (самокорекції, взаємокорекції) за ефективністю навчально-пізнавальної діяльності:

Засобами оцінювання результатів навчання є:

- модульні контрольні роботи;
- звіти з лабораторних робіт;

- командні проєкти; індивідуальні та групові завдання;
- завдання на лабораторному обладнанні;
- захист курсової роботи;
- екзаменаційна робота;
- комплексна контрольна робота (за необхідністю).

Методами демонстрування результатів навчання є:

- усні відповіді;
- письмові відповіді;
- виконання завдань із застосуванням комп'ютерної техніки;
- оформлення звітів з лабораторних робіт;
- презентації результатів виконаних завдань та досліджень.

Допускається застосування дистанційних технологій для діагностики результатів навчання.

7. Форми поточного та підсумкового контролю

Досягнення здобувача вищої освіти оцінюються за 100-бальною системою Університету.

Поточний контроль проводиться в межах навчальних занять і передбачає оцінювання теоретичної підготовки здобувачів вищої освіти із зазначених тем (у тому числі, самостійно опрацьованого матеріалу) та практичних навичок, набутих під час виконання лабораторних робіт.

Поточний контроль здійснюється протягом семестру в наступних формах:

- перевірка екзаменаційних робіт;
- перевірка та захист звітів з лабораторних робіт;
- проведення та перевірка модульних контрольних робіт;
- контроль виконання розділів індивідуального науково-дослідного завдання;
- контрольна робота на заочній формі навчання;
- семестрова атестація;
- перевірка конспекту лекцій;
- контроль відвідування занять.

Перевірка звіту з лабораторної роботи включає оцінювання правильності та повноти виконання завдання, правильності та повноти висновків, правильності оформлення звіту.

Процедура захисту звіту з лабораторної роботи включає один або декілька елементів:

- письмове викладення відповідей на запитання за тематикою роботи;
- усне опитування за тематикою роботи;
- виконання завдань із застосуванням комп'ютерної техніки.

При виконанні модульних контрольних робіт здобувач вищої освіти відтворює засвоєні знання шляхом надання письмових відповідей на поставлені

запитання. На теоретичні запитання необхідно давати розгорнуті відповіді, супроводжуючи їх прикладами та ілюстраціями. Повнота відповідей оцінюється згідно з теоретичним матеріалом, наведеним у джерелах інформації для кожної теми. На тестові запитання потрібно вказати номер правильної відповіді та її формулювання.

Контрольна робота на заочній формі навчання за змістом є об'єднаним представленням модульних контрольних робіт, які проводяться для здобувачів денної форми навчання, і має відповідати тим самим вимогам. Контрольна робота на заочній формі навчання виконується протягом семестру і здається до проведення підсумкового контролю.

Поточний модульний контроль проводиться з урахуванням даних поточного контролю за відповідний змістовний модуль і має на меті оцінку результатів знань студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля.

Процедура захисту звіту з індивідуального науково-дослідного завдання (курсової роботи) включає наступні елементи:

- надання пояснювальної записки звіту з індивідуального науково-дослідного завдання (курсової роботи) в електронному вигляді;
- усне опитування за тематикою роботи;
- виконання завдань із застосуванням комп'ютерної техніки.

Семестрова атестація дає змогу здійснити проміжну оцінку досягнень здобувача вищої освіти. В період семестрової атестації викладач оцінює результати поточного контролю та атестує чи не атестує здобувача вищої освіти.

За рішенням кафедри студентам, які брали участь у науково-дослідній роботі – роботі конференцій, студентських наукових гуртків, підготовці публікацій, а також були учасниками олімпіад, конкурсів, тощо можуть присуджуватися додаткові бали. Додаткові бали також можуть присуджуватися за результатами перевірки конспекту лекцій, контролю відвідування занять та за активність на лекціях і практичних заняттях.

За всі поточні контрольні заходи протягом семестру, з урахуванням додаткових балів, студент сумарно може отримати від 0 до 100 балів.

Умовою допуску студента до семестрового підсумкового контролю є мінімальна сума у 60 балів, яку студент повинен набрати у разі виконання всіх елементів модулів.

Семестровий підсумковий контроль з дисципліни проводиться відповідно до навчального плану у вигляді **екзамену** в терміни, встановлені графіком навчального процесу, та в обсязі навчального матеріалу, визначеному робочою програмою навчальної дисципліни.

Студент, який набрав за всі поточні контрольні заходи менше 60 балів або хоче отримати додаткові бали, пише семестрову екзаменаційну роботу (проводиться у письмовій формі), до якої він допускається, якщо захистив курсову роботу і має за виконання всіх передбачених елементів модулів не

менше 35 балів. Максимальна кількість балів за семестрову підсумкову залікову роботу (екзамен) становить 40 балів. Студенти заочної форми навчання пишуть підсумкову залікову роботу обов'язково.

Підсумкова оцінка з дисципліни від 60 до 100 балів визначається як сума балів за змістовими модулями та семестрової залікової роботи (у разі її написання).

Зарахування кредитів навчального курсу можливо тільки після досягнення результатів, запланованих РПНД, що виражається в одній з позитивних оцінок, передбачених чинним законодавством.

8. Критерії оцінювання результатів навчання

8.1 Критерії оцінювання лабораторних робіт

При оцінюванні лабораторних робіт враховуються наступні критерії:

- виконання роботи та правильність виконання;
- наявність звіту, вчасність подачі та якість звіту;
- захист звіту.

Максимальна оцінка за кожну лабораторну роботу для студентів ДФН:

- у четвертому семестрі – 5 балів,
- у п'ятому семестрі – 2 бали.

Максимальна оцінка за кожну лабораторну роботу для студентів ЗФН:

- у четвертому семестрі – 15 балів,
- у п'ятому семестрі – 15 балів.

Максимальна сумарна кількість балів за лабораторні роботи для студентів ДФН становить:

- у четвертому семестрі: $8 \times 5 = 40$ балів;
- у п'ятому семестрі: $15 \times 2 = 30$ балів.

Максимальна сумарна кількість балів за лабораторні роботи для студентів ЗФН становить:

- у четвертому семестрі: $2 \times 15 = 30$ балів;
- у п'ятому семестрі: $2 \times 15 = 30$ балів.

Критерії оцінювання лабораторних робіт

Кількість балів (в дужках для ЗФН)	Критерії оцінювання
М1	
5 (15)	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Студент надав правильні відповіді на всі питання захисту.

Кількість балів (в дужках для ЗФН)	Критерії оцінювання
4 (12)	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках. Студент надав принципово правильні відповіді на питання захисту (без суттєвих помилок).
3 (9)	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Студент відповів на питання захисту частково чи з принциповими помилками.
2 (6)	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.
1 (3)	Завдання виконано не у повному об'ємі (не менше 70%). Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.
0 (0)	Робота не виконана.
	<i>Максимальна сумарна оцінка студента за даний компонент програми для ДФН – 40 балів (8 робіт по 5 балів). Максимальна сумарна оцінка студента за даний компонент програми для ЗФН – 30 балів (2 роботи по 15 балів). При незначних відхиленнях від вказаних критеріїв оцінка може доповнюватись знаками «-» або «+», що при підсумовуванні відповідає 0,5 бала.</i>
М2	
2 (15)	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Студент надав правильні відповіді на всі питання захисту.
1,6 (12)	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках. Студент надав принципово правильні відповіді на питання захисту (без суттєвих помилок).
1,2 (9)	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Студент відповів на питання захисту частково чи з принциповими помилками.
0,8 (6)	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.
0,4 (3)	Завдання виконано не у повному об'ємі (не менше 70%). Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.
0 (0)	Робота не виконана.
	<i>Максимальна сумарна оцінка студента за даний компонент програми для ДФН – 30 балів (15 робіт по 2 бали). Максимальна сумарна оцінка студента за даний компонент програми для ЗФН – 30 балів (2 роботи по 15 балів). При незначних відхиленнях від вказаних критеріїв оцінка може доповнюватись знаками «-» або «+», що при підсумовуванні відповідає 0,2 бала.</i>

8.2 Критерії оцінювання модульних контрольних робіт

Для поточного модульного контролю студентами виконуються 6 (шість) модульних контрольних роботи за матеріалами змістовних модулів. Критерієм оцінювання МКР є відсоток правильних відповідей на питання МКР.

Максимальна кількість балів за кожну МКР для студентів ДФН:

- у четвертому семестрі: 10 балів;
- у п'ятому семестрі: 15 балів.

Загальна сума балів за модульні контрольні роботи для студентів ДФН:

- у четвертому семестрі: $2 \times 10 = 20$ балів;
- у п'ятому семестрі: $2 \times 15 = 30$ балів.

Максимальна кількість балів за кожну МКР для студентів ЗФН:

- у четвертому семестрі: 15 балів;
- у п'ятому семестрі: 15 балів.

Загальна сума балів за модульні контрольні роботи для студентів ЗФН:

- у четвертому семестрі: $2 \times 15 = 30$ балів;
- у п'ятому семестрі: $2 \times 15 = 30$ балів.

Критерії оцінювання задач та практичних завдань в МКР для ДФН

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал (М1)	10	9	8	7	6	5	4	3	2	1
Бал (М2)	15	13,5	12	10,5	9	7,5	6	4,5	3	1,5

Критерії оцінювання задач та практичних завдань в МКР для ЗФН

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал (М1)	15	13,5	12	10,5	9	7,5	6	4,5	3	1,5
Бал (М2)	15	13,5	12	10,5	9	7,5	6	4,5	3	1,5

8.3 Критерії оцінювання курсової роботи

Критеріями оцінювання курсової роботи є:

- самостійність виконання завдання;
- правильність виконання завдання;
- вчасність оформлення звіту з курсової роботи;
- правильність оформлення звіту з курсової роботи;
- правильність відповідей на питання при захисті курсової роботи.

Максимальна кількість балів за курсову роботу становить 100 балів.

Розподіл максимально можливої кількості балів за курсову роботу

Звіт з курсової роботи	Захист курсової роботи	Сума
50	50	100

Критерії оцінювання пояснювальної записки і графічної частини курсової роботи

виконання роботи, %	Критерії оцінювання пояснювальної записки і графічної частини курсової роботи	бал
100	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Графічна частина виконана відповідно до вимог.	50
70 - 99	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках і/або у графічній частині курсової роботи.	40
59 - 69	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Графічна частина містить незначні некоректності в оформленні.	30
40 - 58	Завдання виконано у повному об'ємі але з помилками. Звіт (в тому числі графічна частина) містить неточності у висновках та окремі помилки.	20
20 - 39	Завдання виконано не у повному об'ємі. Надано звіт, що містить неточності і помилки. Графічна частина містить помилки.	10
1 - 20	Робота не виконана.	0

Критерії оцінювання захисту курсової роботи

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	50	45	40	35	30	25	20	15	10	5

8.4 Критерії оцінювання екзаменаційної роботи

Максимальна оцінка за екзаменаційні роботи – 40 балів.

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	40	36	32	28	24	20	16	12	8	4

Рівні підсумкової оцінки екзамену з дисципліни (перерахунковий коефіцієнт – 0,4)

Оцінка за 100-бальною шкалою університету / Grade according to 100-points scale of University	Оцінка за шкалою ЄКТС / Grade according to ECTS scale
90-100 (творчий рівень)/(creative level)	A (відмінно) / (excellent)
82-89 (високий рівень)/(high level)	B (дуже добре) / (very good)

Оцінка за 100-бальною шкалою університету / Grade according to 100-points scale of University	Оцінка за шкалою ЄКТС / Grade according to ECTS scale
74-81 (добрий рівень)/(good level)	C (добре) / (good)
64-73 (середній рівень)/(average level)	D (посередньо) / (average)
60-63 (задовільний рівень)/(satisfactory level)	E (достатньо) / (satisfactory)
35-59 (низький рівень)/(low level)	FX (незадовільно з можливістю повторного складання) / (unsatisfactory with the possibility to repass the exam)
1-34 (незадовільний рівень)/(unsatisfactory level)	F (незадовільно з обов'язковим повторним вивченням) / (unsatisfactory with the compulsory repeating of the course)

8.5 Розподіл балів

Розподіл оцінки за змістовними модулями та видами контролю

		Денна форма		Заочна форма	
		Вид роботи	Кількість балів	Вид роботи	Кількість балів
М1					
ЗМ1	T1	-	0	-	-
	T2	Лабораторна робота 1	5	-	
	T3	-	-	-	-
	T4	Лабораторна робота 2	5	Лабораторна робота 2	15
	МКР1	Тест	10	Тест	15
ЗМ2	T5	Лабораторні роботи 3, 4	10	-	-
	T6	Лабораторна робота 5	5	Лабораторна робота 5	15
	T7	Лабораторна робота 6	5	-	-
	T8	Лабораторні роботи 7, 8	10	-	-
	МКР2	Тест	10	Тест	15
Підсумковий семестровий контроль		екзамен	40	екзамен	40
Всього			100	100	
М2					
ЗМ3	T9	Лабораторна робота 9	2	-	-
	T10	Лабораторні роботи 10, 11, 12, 13	8	Лабораторна робота 10	15
	T11	Лабораторна робота 14	2	-	-
	T12	Лабораторні роботи 15, 16	4	-	-
	МКР3	Тест	15	Тест	15

		Денна форма		Заочна форма	
		Вид роботи	Кількість балів	Вид роботи	Кількість балів
ЗМ4	T13	Лабораторна робота 17	2	-	-
	T14	Лабораторні роботи 18, 19, 20	6	-	-
	T15	Лабораторні роботи 21, 22, 23	6	Лабораторна робота 21	15
	МКР4	Тест	15	Тест	15
Підсумковий семестровий контроль		екзамен	40	екзамен	40
Всього			100	100	

9. Засоби навчання

Апаратне забезпечення, необхідне для вивчення навчальної дисципліни, включає персональний комп'ютер (настільний або ноутбук) із доступом до Інтернет.

Програмне забезпечення, необхідне для вивчення навчальної дисципліни, включає: операційну систему (Windows); програмне забезпечення для інженерних розрахунків ризиків (Excel, Mathcad); текстовий редактор та редактор растрових зображень (для підготовки звітів з лабораторних робіт); pdf-, djv-переглядач (для ознайомлення з джерелами інформації, представленими в електронному вигляді); браузер для доступу до Інтернет-ресурсів.

При очній формі навчання використовуються апаратні та програмні можливості лабораторій №129 і №130 кафедри КТІБ ННІАЕ НУК.

При дистанційній формі навчання використовуються апаратні та програмні можливості домашніх персональних комп'ютерів (настільних комп'ютерів або ноутбуків) та мобільних пристроїв із доступом до Інтернет. Заняття проводиться в Zoom. Необхідна студентам інформація (робоча програма дисципліни, методичні вказівки, рекомендована література, інформація щодо поточної набраної кількості балів) викладається на google-диск кафедри КТІБ, до якого студенти отримують доступ без права редагування. Виконані студентами роботи надсилаються на кафедральну пошту ktib@nuos.edu.ua. Під час воєнного стану допускається виконання звітів з лабораторних робіт і модульних контрольних робіт в рукописному вигляді без дотримання стандартів оформлення. Такі звіти надсилаються у вигляді графічних зображень (фотографій). Відповідно, для дистанційної форми навчання додатково використовуються Zoom, e-mail і відеокамери мобільних пристроїв.

10. Рекомендовані джерела інформації

Основна література

Навчально-методична література

1. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]. / В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа. – Львів.: «Магнолія 2006», 2018. – 320 с. URL: <https://spadok.org.ua/books/Buryachok-Osnovy-info-ta-ciberbezpeky.pdf>
2. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок, Р. В. Киричок, П. М. Складанний – К., 2019. – 320 с.
3. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня., Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. - 128 с.
4. Гапак О. М., Глебена М. І. Захист інформації в комп'ютерних системах. – Ужгород: УЖНУ, 2021. – 184 с.
5. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. Посібник. - Дніпро: Дніпропетровський держ. ун-т внутріш. справ, 2020. – 144 с.
6. Мельник А. Архітектура комп'ютера: підручник. – Луцьк: Волинська обл. друкарня, 2008. – 470 с.
7. Опорний конспект лекцій з дисципліни «Системи технічного захисту інформації». Вінниця: ВНТУ, 2017. – 61 с. URL: https://zi.vntu.edu.ua/uploads/NMKD///STZI/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B8%20%D1%82%D0%B5%D1%85%D0%BD%D1%96%D1%87%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97/%D0%9A%D0%9B%D0%9C_%D0%BA%D0%BE%D0%BD%D1%81%D0%BF%D0%B5%D0%BA%D1%82%20%D0%A1%D0%A2%D0%97%D0%86.pdf
8. Ромака В. А. та ін. Системи менеджменту інформаційної безпеки : навч. посібник. -Львів : Вид-во Львів політехніки, 2012. – 232 с.

Нормативно-правова база

Закони України:

9. Доктрина інформаційної безпеки України. URL: <https://www.president.gov.ua/documents/472017-21374>
10. Закон України «Про банки і банківську діяльність». URL <http://zakon2.rada.gov.ua/laws/show/2121-14>.
11. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України». URL: <http://zakon2.rada.gov.ua/laws/show/3475-15>.

12.Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»/ URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>

13.Закон України «Про захист персональних даних» URL: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297-17>

14.Закон України «Про інформацію». URL <http://zakon2.rada.gov.ua/laws/show/2657-12>.

15.Закон України „Про ліцензування певних видів господарської діяльності”. URL: <https://zakon.rada.gov.ua/laws/show/222-19#Text>

16.Закон України «Про Національний банк України». URL <http://zakon3.rada.gov.ua/laws/show/679-14>.

17.Закон України «Про платіжні системи та переказ коштів в Україні». URL <http://zakon3.rada.gov.ua/laws/show /2346-14/ed20120527>

18.Закон України «Про основні засади забезпечення кібербезпеки України» URL : <http://zakon.rada.gov.ua/laws/show/2163-19>

19.Звід відомостей, що становлять державну таємницю URL: <https://zakon.rada.gov.ua/laws/show/z0052-21#Text>

20.Стратегія кібербезпеки України URL: <https://zakon.rada.gov.ua/laws/show/96/2016#Text>

21.Указ Президента України від 27.09. 99 № 1229 “Про затвердження Положення про технічний захист інформації в Україні”. URL: <https://zakon.rada.gov.ua/laws/show/1229/99#Text>

Міжнародні нормативні документи:

22.CSC-STD-001-83. Trusted Computer System Evaluation Criteria. URL: <https://www.cs.cmu.edu/afs/cs/usr/bsy /security/CSC-STD-001-83.txt>.

23.CSC-STD-003-85 Guidance for applying the Department of Defence Trusted Computer System Evaluation Criteria in specific environment. URL: http://www.cbi.umn.edu/securitywiki/pub/CBI_ComputerSecurity/PubRainbowSeries/csc-std-003-85lightyellow.pdf

24.CTCPEC. Canadian Trusted Computer Product Evaluation Criteria. URL: http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/kanadskie_kriterii_bezopasnosti_kompjuternyx_sistem_ctcpec.

25.Information Technology Security Evaluation Criteria URL: https://www.bsi.bund.de/shareddocs/downloads/de/bsi/zertifizierung/interpretationen/ais_18_itsec_jil_e_pdf.pdf?_blob=publicationfile.

26.ISO/IEC 9001:2000 Quality management systems. Requirements. URL : <https://www.iso.org/standard/21823.html>.

27.ISO/IEC 14001:2015Environmental management systems. Requirements with guidance for use. URL: <https://www.iso.org/standard/60857.html>

28.ISO/IEC 15408-1:2009. Informational technology. Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model. URL: <https://www.iso.org/standard/50341.html>

29.ISO/IEC 15408-2:2008. Informational technology. – Security techniques – Evaluation criteria for IT security. – Part 2: Security functional requirements. URL: <https://www.iso.org/standard/46414.html>

30.ISO/IEC 15408-3:2008. Informational technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirement. URL: <https://www.iso.org/standard/46413.html>

31.ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management. URL: <https://www.iso.org/standard/39612.html>.

32.ISO/IEC 18045:2005. Informational technology – Security techniques – Methodology for IT security evaluation.

33.ISO/IEC 27001:13Information technology. Security techniques. Information security management systems. Requirements. URL: <https://www.iso.org/standard/54534.html>.

34.ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls. URL: <https://www.iso.org/ru/standard/54533.html>

35.ISO 27005:2018 Information technology -- Security techniques -- Information security risk management. URL: <https://www.iso.org/standard/75281.html>

36.Federal Information Processing Standards. URL: <http://csrc.nist.gov/publications/PubsFIPS.html>.

37.NCSC-TG-001A Guide to Understanding Audit in Trusted Systems. URL: <https://fas.org/irp/nsa/rainbow/tg001.htm>.

38.NCSC-TG-003A guide to understanding discretionary access control in trusted systems. URL: <http://csrc.nist.gov/publications/secpubs/rainbow/tg003.txt>.

39.NCSC-TG-005Trusted Network Interpretation. URL: <http://www.filewatcher.com/m/NCSC-TG-005.pdf.1290550-0.html>.

40.NCSC-TG-006-88Guide to understanding configuration management in trusted systems. URL: <https://fas.org/irp/nsa/rainbow/tg006.htm>.

41.NCSC-TG-007-95A Guide to Understanding Design Documentation in Trusted. URL: <http://ftp.mirrorservice.org/sites/ftp.wiretapped.net/pub/security/info/reference/rainbow-books/NCSC-TG-007.pdf>.

42.NCSC-TG-021Trusted Database Management System Interpretation. URL: http://www.cbi.umn.edu/securitywiki/pub/CBI_Computer_Security/PubRainbowSeries/ncsc-tg-021purple.pdf.

Нормативні документи системи ТЗІ України:

43.ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення. URL: <http://metrology.com.ua/download/dstu-gost-gost-r/60-dstu/441-dstu-3396-0-96>.

44.НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: <https://tzi.com.ua/downloads/1.1-003-99.pdf>.

45.НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі URL: <https://tzi.com.ua/downloads/1.4-001-2000.pdf>

46.НДТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Електронний ресурс] – Режим доступу: <http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342>

47.НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.- URL: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article;jsessionid=afd6198c23cb1f96abafd7189bbdce03?showhidden=1&art_id=101870&cat_id=89734&ctime=1344501089407.

48.НД ТЗІ 2.5-008-02 "Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2". URL: <http://info-stand.com/nb-ukraine/by-type/nd-tzi/22-ndtzi25-008-02.html>.

49.НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. URL: <http://www.dsszzi.gov.ua%2fdstszi%2fdoccatalog%2fdocument%3fid%3d41647&ei=guz5uk3xg8z3sga4r4cwcq&usg=afqjcnfy e5kjfdqsympy-ekqedagtercmw&cad=rja>.

50.НД ТЗІ 2.6-001-11 «Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах». URL: <http://dstszi.kmu.gov.ua/dstszi/doccatalog/document;jsessionid=62556e8a1a8a5363657e5da67bfce233?id=103245>

51.НД ТЗІ 2.6-002-2015 Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99. URL : http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89740.

52.НД ТЗІ 2.6-003-2015 Порядок зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89740.

53.НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу. – К. : Адміністрація держспецзв'язку, 2009. – 171 с. - URL: <http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=103246>.

54.НДТЗІ 2.7-010-09. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу. – К.: Адміністраціядержспецзв'язку, 2009. –131 с. URL: <https://tzi.com.ua/downloads/2.7-010-09.pdf>

55.НД ТЗІ 2.7-013-2016 Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого

доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99. URL : http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89740.

56.НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». URL: <https://tzi.com.ua/downloads/3.7-003-2005.pdf>

57.Організація реагування на інциденти та обробка інцидентів безпеки: Керівництво для організації електрозв'язку. Рекомендація МСЭ-Т E.409 (ITU-T E.409). – Женева, 2004. URL: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.409-200405-I!!PDF-E&type=items

58.Положення про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України. URL : <http://bank.gov.ua/doccatalog/document?id=22694128>.

59.Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, затверджений постановою №1295 Кабінету міністрів України від 23.12.2020. URL: <https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF>

60.Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.06 № 373. URL: <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text>

61.Правила організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України. URL : <http://zakon2.rada.gov.ua/laws/show/z0419-07>.

62.Р–СП Рекомендації з технічного захисту інформації в приміщеннях серверних, електронної пошти та інших спеціальних приміщень. - К.:ТОВ “НікС”, 2003. - 25 с.

63.СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності, система управління інформаційною безпекою. Вимоги»/ URL : <http://www.bank.gov.ua/doccatalog/document?id=72235>.

64.СОУ Н НБУ 65.1 СУІБ 2.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» URL : <https://kyianyn.files.wordpress.com/2010/12/nbu-27002.pdf>.

Допоміжна література

Навчально-методична література

1. Архіпов А.Є, Архіпова Є.О. Особливості визначення обсягу інвестицій в систему захисту інформаційних ресурсів // Інвестиції: практика та досвід. – 2015/ - № 11. – С.71-74.

2. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко – К. : ДУТ - КНУ, 2016. – 178 с.

3. Гайвороновський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. - К.: Видавнича група BVH, 2009
4. Голубів В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій : навч. посібник. -Запоріжжя : ГУ "ЗІДМУ", 2002
5. Горохов С.М., Кондратьєва Н. В., Кононович В.Г., Стайкуца С.В. Програми та методики державної експертизи інформаційної захищеності телекомунікацій. -Одеса: ОНАЗ ім. О.С. Попова, 2013
6. Домарев В.В., Домарев Д.В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) – Донецьк: Велстар, 2012. – 146 с.
7. Корченко А.Г., Архипов А.Е., Казимирчук С.В. Анализ и оценивание рисков информации безопасности. - К.: ООО «Полиграф-Лазурит», 2013. – 275 с.
8. Корченко О.Г., Гнатюк С.О, Казмірчук С.В., Панченко В.М., Мельник С.В. Аудит та управління інцидентами інформаційної безпеки. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.
9. Кукарін О.Б. Електронний документообіг та захист інформації: Навчальний посібник. -К.: НАДУ, 2015
10. Логінова Н.І., Дробожур Р.Р. Правовий захист інформації: Навчальний посібник. -Одеса: Фенікс, 2015

Нормативно-правова база

Закони України:

11. Закон України «Про державну таємницю». URL: <http://zakon.rada.gov.ua/laws/show/3855-12>
12. Закон України „Про доступ до публічної інформації”. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
13. Закон України „Про оперативно-розшукову діяльність”. URL: <https://zakon.rada.gov.ua/laws/show/2135-12#Text>
14. Закон України «Про основи національної безпеки України» URL: <http://zakon.rada.gov.ua/laws/show/2469-19>
15. Закон України „Про Раду національної безпеки і оборони України”. URL: <https://zakon.rada.gov.ua/go/183/98-%D0%B2%D1%80>
16. Закон України „Про розвідку”. URL: <https://zakon.rada.gov.ua/laws/show/912-20#Text>
17. Закон України „Про службу безпеки України”. URL: <https://zakon.rada.gov.ua/laws/show/2229-12#Text>
18. Закон України „Про Службу зовнішньої розвідки України”. URL: <https://zakon.rada.gov.ua/laws/show/3160-15#Text>
19. Закон України «Про технічні регламенти та оцінку відповідності». URL : <http://zakon5.rada.gov.ua/laws/show/124-19>.

Нормативні документи системи ТЗІ України:

20.ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. URL : <http://metrology.com.ua/download/dstu-gost-gost-r/60-dstu/440-dstu-3396-1-96>.

21.ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. URL: <http://www.dut.edu.ua/ru/lib/60/category/925/view/1045>.

22.Наказ №45 Адміністрації ДССЗІ 26.03.2007 «Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації». URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=50825&cat_id=38835

23.НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. URL: http://www.dut.edu.ua/uploads/1_1027_69115427.pdf.

24.НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: <http://www.afa.biz.ua/documents/31-infobezopasnot/33-what-is-uncategorised-article?format=pdf>.

25.НД ТЗІ 1.1-004-2003 Протидія технічним розвідкам. Терміни та визначення. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article%3Bjsessionid=9082A42798BC38188D392292242BFBA2?showHidden=1&art_id=102366&cat_id=89734&ctime=1344587370607.

26.НД ТЗІ 2.5-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту. URL: <http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=103243>

27.НД ТЗІ 2.5-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту. URL: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=101820&cat_id=89734&ctime=1344500798284.

28.НД ТЗІ 2.5-003-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту. URL: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=101836&cat_id=89734&ctime=1344500934167.

29.НД ТЗІ 2.7-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт. -К.:ТОВ "НікС", 1999. – 54 с.

30.НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки. URL: <http://www.dsszzi.gov.ua/dsszzi/>

control/uk/publish/article?showHidden=1&art_id=102299&cat_id=46556&ctime=1344510938381.

31.НД ТЗІ 2.7-008-08 Захист інформації на об'єктах інформаційної діяльності. Вимоги та рекомендації із забезпечення захисту мовної інформації від витоку акустичним та віброакустичним каналами. Методичні вказівки. URL : https://tzi.ua/ua/nd_tz_2.5-008-2002.html.

32.НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова). URL: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=102205&cat_id=46556&ctime=1344503878438.

33.Положення про державну експертизу в сфері технічного захисту інформації. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.2007 № 93 Зареєстровано в Міністерстві юстиції України 16.07.2007 за № 820/14087 із змінами, затвердженими наказом Адміністрації Держспецзв'язку від 10.10.2012 № 567, зареєстрованим в Міністерстві юстиції України 06.11.2012 за № 1863/22175 URL: <http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=105528>.

Інформаційні ресурси в Інтернеті

1. Верховна Рада України. Законодавство України. URL: <http://zakon.rada.gov.ua/laws/>

2. Державна служба спеціального зв'язку та захисту інформації. URL: <https://cip.gov.ua/ua>

3. Команда реагування на комп'ютерні надзвичайні події України. URL: <https://cert.gov.ua/>

4. Нормативна база у сфері ТЗІ URL: <http://altersign.com.ua/korysna-informacija/normativna-baza-u-sferi-tzi>

5. Офіційний сайт ISO. URL: <https://www.iso.org/standard>

6. Портал безпека. URL: <https://www.bezpeka.com/uk/golovna/>

7. Системи онлайн-освіти. URL: <https://prometheus.org.ua/>, <https://www.coursera.org>, <http://www.udacity.com>

Зміни та доповнення