

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 ОПП
ОК34



ЗАТВЕРДЖУЮ

Проректор з науково-педагогічної
роботи, к.т.н., доцент

С.О. Слободян

«___» _____ 2022 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 2022 рік

Робоча програма навчальної дисципліни «Управління інформаційною безпекою» є однією із складових комплексної підготовки фахівців галузі знань 15 «Автоматизація та приладобудування», спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології», освітня програма «Комп'ютерно-інтегровані технології та системи автоматизації»
«__» _____ 2022 р. – 23 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 «Комп'ютерно-інтегровані технології та системи автоматизації»
Вінниченко І.Л., доцент кафедри комп'ютеризованих систем управління, канд. техн. наук, доцент

Проект робочої програми навчальної дисципліни «Безпека інформаційних та комунікаційних систем» розглянуто на засіданні кафедри КСУ.
Протокол від «26» _____ 09 _____ 2022 р. № 2.

Завідувач кафедри КСУ, д.т.н., доцент _____ О.О. Черно

Проект робочої програми навчальної дисципліни «Управління інформаційною безпекою» розглянуто методичною радою Навчально-наукового інституту автоматики та електротехніки.
Протокол від «20» _____ 10 _____ 2022 р. № 3.

Голова _____

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 «26» _____ 10 _____ 2022 р. № 8.

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	6
4. Очікувані результати навчання	7
5. Програма навчальної дисципліни	7
6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування.....	11
7. Форми поточного та підсумкового контролю	12
8. Критерії оцінювання результатів навчання.....	14
9. Засоби навчання	16
10. Рекомендовані джерела інформації.....	17

ВСТУП

Анотація

Навчальна дисципліна «Управління інформаційною безпекою» є дисципліною професійної підготовки бакалаврів зі спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології». Дана дисципліна є обов'язковим компонентом освітньої програми, який забезпечує теоретичну та практичну підготовку студентів до вирішення питань захисту інформації в автоматизованих системах, 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 151 "Automation and computer-integrated technologies". This discipline is a mandatory component of the educational program, which provides theoretical and practical training of students to solve information protection issues in automated systems, 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 – 3	Галузь знань 15 «Автоматизація та приладобудування» Спеціальність: 151 «Автоматизація та комп'ютерно-інтегровані технології»	Обов'язкова	
Модулів – 1	Освітня програма «Комп'ютерно-інтегровані технології та системи автоматизації»	Рік підготовки	
Змістових модулів – 2		2-й	2-й
		Семестр	
Загальна кількість годин – 90		4-й	4-й
Тижневих годин для денної форми навчання: Аудиторних – 2; Самостійної роботи: – 4.	Рівень вищої освіти: перший (бакалаврський)	Лекції, год	
		15 год.	4 год.
		Лабораторні роботи, год.	
		15 год.	4 год.
		Практичні роботи, год.	
		-	-
		Самостійна робота, год.	
		60	82
		Вид контролю: 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.

- (ЗК4) - Навички використання інформаційних і комунікаційних технологій;
- (ФК9) - Здатність вільно користуватись сучасними комп'ютерними та інформаційними технологіями для вирішення професійних завдань, програмувати та використовувати прикладні та спеціалізовані комп'ютерно-інтегровані середовища для вирішення задач автоматизації.

3. Передумови для вивчення навчальної дисципліни

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

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

4. Очікувані результати навчання

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

– (ПРН4) - Розуміти суть процесів, що відбуваються в об'єктах автоматизації (за галузями діяльності) та вміти проводити аналіз об'єктів автоматизації і обґрунтовувати вибір структури, алгоритмів та схем керування ними на основі результатів дослідження їх властивостей.

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; [18]; [19].

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]; [10-13]; [14-17].

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; [17]

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

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	90	15	15	60	90	4	4	82

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	-
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		15	4

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.

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 екзамену – 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 екзамену – 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 відеорядом	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
Разом		12	12

Розподіл годин підготовки самостійної роботи

№	Вид роботи	Кількість годин	
		ДНФ	ЗНФ
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
Разом		60	82

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;
- 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;
- 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.

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 має за виконання всіх передбачених елементів модулів не менше 35 балів. Максимальна кількість балів за семестрову підсумкову екзаменаційну роботу (екзамен) становить 40 балів. Студенти заочної форми навчання пишуть підсумкову екзаменаційну роботу обов'язково.

Підсумкова оцінка з дисципліни від 60 до 100 балів визначається як сума балів за змістовими модулями та семестрової екзаменаційної 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

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 становить:

- для студентів ДФН: 5 балів;
- для студентів ЗФН: 15 балів.

Максимальна сумарна кількість балів за лабораторні роботи для студентів становить:

- для ДФН: $8 \times 5 = 40$ балів;
- для ЗФН: $2 \times 15 = 30$ 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.
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>

Для поточного модульного контролю студентами виконуються дві модульні контрольні роботи за матеріалами змістовних модулів. Критерієм оцінювання МКР є відсоток правильних відповідей на питання МКР.

Максимальна кількість балів за кожну МКР становить:

- для студентів ДФН: 10 балів;
- для студентів ЗФН: 15 балів.

Загальна сума балів за модульні контрольні роботи становить:

- для студентів ДФН: $2 \times 10 = 20$ балів;
- для студентів ЗФН: $2 \times 15 = 30$ балів.

Критерії оцінювання задач та практичних завдань в МКР для ДФН

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	10	9	8	7	6	5	4	3	2	1

Критерії оцінювання задач та практичних завдань в МКР для ЗФН

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

Критерієм оцінювання екзаменаційної роботи є відсоток правильних повних відповідей на питання білету.

Максимальна оцінка за екзаменаційну роботу – 40 балів.

Критерії оцінювання екзаменаційної роботи

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)
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)

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	

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 Державну службу спеціального зв'язку та захисту інформації України». URL: <http://zakon2.rada.gov.ua/laws/show/3475-15>.

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

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

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

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

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

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

17.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>

Нормативні документи системи ТЗІ України:

18.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>.

19.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>.

Допоміжна література

Навчально-методична література

1. 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.

2. Гайвороновський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. - К.: Видавнича група BVH, 2009
3. 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
4. Корченко А.Г., Архипов А.Е., Казимирчук С.В. Анализ и оценивание рисков информации безопасности. - К.: ООО «Полиграф-Лазурит», 2013. – 275 с.
5. 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.
6. Кукарін О.Б. Електронний документообіг та захист інформації: Навчальний посібник. -К.: НАДУ, 2015
7. Логінова Н.І., Дробожур Р.Р. Правовий захист інформації: Навчальний посібник. -Одеса: Фенікс, 2015

Нормативно-правова база

Закони України:

8. Закон України «Про державну таємницю» URL : <http://zakon.rada.gov.ua/laws/show/3855-12>
9. Закон України „Про доступ до публічної інформації”
- 10.Закон України «Про основи національної безпеки України» URL : <http://zakon.rada.gov.ua/laws/show/2469-19>
- 11.Закон України „Про службу безпеки України”. URL: <https://zakon.rada.gov.ua/laws/show/2229-12#Text>
- 12.Закон України «Про технічні регламенти та оцінку відповідності». URL: <http://zakon5.rada.gov.ua/laws/show/124-19>.

Міжнародні нормативні документи:

- 13.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>.
- 14.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
- 15.CTCPEC. Canadian Trusted Computer Product Evaluation Criteria. URL: http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio_kanadskie_kriterii_bezopasnosti_kompjuternyx_sistem_ctcpec.
- 16.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.

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

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

19.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>

20.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>

21.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>

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

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

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

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

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

27.ITU-T Recommendation E.409 (05/2004). Incident organization and security incident handling: Guidelines for telecommunication organizations. Series E: Overall network operation, telephone service, service operation and human factors network management. URL: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.409-200405-I!!PDF-E&type=items

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

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

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

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

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

33.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>.

34.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:

35.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>.

36.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

37.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>.

38.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.

39.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>

40.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.

41.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>.

42.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=afqjcnfye5kjfdqsympy-ekqedagtercmw&cad=rja>.

43.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>

44.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.

45.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>

46.Організація щодо реагування на інциденти та обробка інцидентів безпеки: Керівництво для організації електрозв'язку. Рекомендація МСЭ-Т E.409 (ITU-T E.409). – [Чинний від 2004-28-05]. — Женева, 2004. – С. 13-22 – (Рекомендація Міжнародної організації телекомунікацій).

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

48.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>

49.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>

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