ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету IT
_____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
«31» 08 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Функційна безпека інформаційних та комп'ютерних систем

Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека та захист інформації
Рівень вищої освіти	Другий магістерський
Освітньо-професійна програма	Кібербезпека та захист інформації
Обсяг дисципліни	8 кредитів ЄКТС
Шифр дисципліни	ВД.05
Мова навчання	Українська
Статус дисципліни	Вибіркова
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Очна (денна)	-	-	8	240	85	36	36	18		155			+	

Робоча програма складена _____ д-р філософії Микола СТЕЦЮК
Підпис(и) автора(ів) Ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 31.08.2023 № 1 Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Олег САВЕНКО .
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2023

ФУНКЦІЙНА БЕЗПЕКА ІНФОРМАЦІЙНО КОМП'ЮТЕРНИХ СИСТЕМ

Тип дисципліни	Вибіркова
Освітній рівень	Другий (магістерський)
Мова викладання	Українська
Семестр	Другий
Кількість встановлених кредитів ЄКТС	5
Форми навчання, для яких викладається дисципліна	Очна денна

Результати навчання. Студент, який успішно завершив вивчення дисципліни, повинен *застосовувати, інтегрувати, розробляти* сучасні інформаційні технології, фізичні та математичні методи в сфері функційної безпеки інформаційно-комп'ютерних систем; *забезпечувати* безперервність бізнес-процесів, *виявляти* уразливості інформаційних систем, *аналізувати* та *оцінювати* ризики для функційної безпеки організації; аналізувати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до стратегії функційної безпеки організації; *аналізувати, розробляти* і *супроводжувати* систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій; досліджувати, *розробляти* та *впроваджувати* методи протидії інцидентам у сфері функційної безпеки, здійснювати процедури управління та розслідування інцидентів; приймати обґрунтовані рішення з питань функційної безпеки у складних умовах; планувати навчання та контролювати роботу з персоналом у напрямку соціотехнічної безпеки; *використовувати* методи комп'ютерного моделювання для дослідження процесів функційної безпеки інформаційно-комп'ютерних систем;

Зміст навчальної дисципліни: Функційна безпека та надійність інформаційно-комп'ютерних систем. Принципи функційної безпеки та проблеми. Основи теорії надійності та математичні основи. Види відмов та аналіз причин. Структурно-логічний аналіз технічних систем та методи аналізу. Показники надійності. Резервування для підвищення функційної безпеки: основи та методи. Розрахунок надійності систем з резервуванням. Випробування на функційну безпеку ІКС: методи та оцінка результатів. Функційна безпека комп'ютерних мереж: загрози та методи захисту. Показники функційної безпеки мереж та методи забезпечення. Функційна безпека програмного забезпечення: проблеми та методи підвищення. Математичні моделі надійності програмних комплексів: теорія масового обслуговування та методи аналізу. Методи оцінки функційної безпеки: статистичні методи та теорія ймовірності. Прогнозування функційної безпеки: математичні методи та практичні підходи. Управління функційною безпекою: методи та системи управління якістю. Інженерні методи підвищення функційної безпеки: підходи та практичні рішення. Аналіз причин функційної безпеки. Оцінка показників функційної безпеки. Моделювання функційної безпеки систем. Аналіз функційної безпеки електронних компонентів. Визначення показників функційної безпеки для інформаційних мереж. Прогнозування функційної безпеки. Управління функційною безпекою. Функційна безпека програмного забезпечення’.

Пререквізити: технології програмування та алгоритмізації, захист інформації в інформаційно-комунікаційних системах, дискретна математика.

Кореквізити: технології та системи захисту інформації, теорія та проєктування захищених систем

Запланована навчальна діяльність: лекцій 36 год., лабораторних робіт 36 год., практичних робіт 18 год. ,самостійної роботи 48 год., разом 138 год.

Форми (методи) навчання: словесні та наочні (лекції); практичні та частково-пошукові (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Форми оцінювання результатів навчання: захист лабораторних робіт, захист практичних робіт ,підсумковий контрольний захід (семестровий контроль).

Вид семестрового контролю: залік.

Навчальні ресурси

1. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах. Одеса: ОНУ, 2020. 350 с.
2. Захист інформації в комп'ютерних системах / І.А. Терейковський, С.О. Гнатюк. Харків: ХНУРЕ, 2020. 300 с.
3. Безпека інформаційно-комунікаційних систем / Грайворонський М.В., Новіков О.М. Київ: КНУ, 2021. 412 с.
4. Safety and Security of Cyber-Physical Systems by Frank J. Furrer, Oliver Goerlitz, Norbert Pohlmann. Springer, 2021. 450 p.
5. Security and Resilience in Cyber-Physical Systems by Masoud Tabib, Mahdi Zareapoor. Elsevier, 2022. 300 p.
6. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua

Викладач: д-р філос. Стецюк М.В.

ВСТУП

Дисципліна «Функційна безпека інформаційно комп’ютерних систем» - складова професійної підготовки магістрів зі спеціальності «Кібербезпека та захист інформації»

Метою дисципліни є формування у майбутніх спеціалістів умінь та компетенцій для забезпечення функціональної безпеки та надійності інформаційно-комп'ютерних систем. Включає аудит, моніторинг та менеджмент безпеки систем; розвиток у студентів фахового стилю мислення; надання глибоких та міцних знань з питань управління інцидентами та ризиками функціональної безпеки в умовах широкого використання сучасних інформаційних технологій.

Предметом дисципліни є сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційно-комп'ютерних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери функціональної безпеки; інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); програмне та програмно-апаратне забезпечення (засоби) для забезпечення функціональної безпеки; системи управління функціональною безпекою; технології, методи, моделі та засоби забезпечення функціональної безпеки; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків).

Завдання дисципліни є забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до освітньо-професійної програми підготовки магістрів зі спеціальності «Кібербезпека та захист інформації»:

компетентності:

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

результати навчання:

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти 4 уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

Студент, який успішно завершив вивчення дисципліни, повинен: застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки; аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту; аналізувати, розробляти і

супроводжувати систему управління інформаційною безпекою організації; забезпечувати безперервність бізнес/операційних процесів, а також аналізувати та оцінювати ризики для інформаційної безпеки організації; досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам; аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій; приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень; планувати навчання, використовувати методи комп‘ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки;

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин відведених на:		
	лекції	**лабораторні роботи**	**самостійну роботу**
Тема 1. Функційна безпека та надійність	8	8	16
Тема 2. Методи аналізу та підвищення функційної безпеки	8	8	18
Тема 3. Практичні аспекти функційної безпеки в ІКС	10	8	20
Тема 4. Прогнозування та управління безпекою	6	8	12
Разом:	**36**	**36**	**48**

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
Тема 1. Функційна безпека та надійність		
1	**Питання та визначення функційної безпеки** 1. Визначення функційної безпеки. 2. Мета функційної безпеки. 3. Принципи функційної безпеки. Літ.: [[1] с.12-25 [2] с.10-30 [3] с.20-40	2
2	**Теорія надійності** 1. Основні поняття надійності. 2. Методи підвищення надійності систем. Літ.: [4] с.34-56 [5] с.40-60 [6] с.50-70	2
3	**Фактори, що впливають на надійність ІКС** 1. Внутрішні фактори. 2. Зовнішні фактори. 3. Вплив людського фактору. Літ.: [2] с.45-60 [8] с.60-75 [7] с.30-50	2
4	**Структурно-логічний аналіз технічних систем** 1. Методи структурного аналізу. 2. Методи логічного аналізу. 3. Аналіз відмов. Літ.: [5] с.70-85 [4] с.90-110 [7] с.40-60	2
Тема 2. Методи аналізу та підвищення функційної безпеки		
5	**Резервування як метод підвищення функційної безпеки** 1. Типи резервування. 2. Переваги резервування. 3. Недоліки резервування. Літ.: [10] с.90-110 [9] с.130-150 [8] с.70-90	2
6	**Розрахунок надійності систем з резервуванням** 1. Методи розрахунку надійності. 2. Приклади розрахунків. Літ.: [9] с.115-130 [8] с.130-145 [6] с.50-70	2
7	**Випробування на функційну безпеку ІКС** 1. Методи випробувань. 2. Аналіз результатів. Літ.: [8] с.140-155 [5] с.155-175 [3] с.80-100	2
8	**Функційна безпека комп'ютерних мереж** 1. Методи забезпечення безпеки мереж. 2. Основні загрози. Літ.: [17] с.160-175 [19] с.175-190 [6] с.90-110	2
Тема 3. Практичні аспекти функційної безпеки в ІКС		
9	**Показники функційної безпеки мереж** 1. Основні показники. 2. Методи вимірювання. Літ.: [19] с.180-195 [4] с.200-220 [3] с.110-130	2
10	Функційна безпека програмного забезпечення1. Категорії аудиту безпеки 1. Методи забезпечення безпеки ПЗ. 2. Аналіз вразливостей. Літ.: Літ.: [18] с.200-215 [2] с.215-230 [7] с.150-170	2

11	**Математичні моделі надійності програмних комплексів** 1. Статистичні моделі. 2. Аналітичні моделі. 3. Оцінка надійності програмного забезпечення. Літ.: Літ.: [9] с.220-235 [1] с.235-250 [7] с.170-190	2
12	**Методи оцінки функційної безпеки** 1. Основні методи оцінки. 2. Практичне застосування. Літ.: [1] с.240-255 [2] с.255-270 [3] с.130-150	2
13	**Прогнозування функційної безпеки** 1. Методи прогнозування. 2. Моделювання надійності. Літ.: [4] с.260-275 [5] с.275-290 [7] с.60-80	2
Тема 4. Прогнозування та управління безпекою		
14	**Управління функційною безпекою** 1. Стратегії управління. 2. Впровадження систем управління. Літ.: [2] с.280-295 [10] с.90-110 [3] с.180-200	2
15	**Оцінка ризиків функційної безпеки** 1. Методи оцінки ризиків. 2. Аналіз ризиків. 3. Управління ризиками. Літ.: [11] с.150-170 [12] с.130-150 [13] с.90-110	2
16	**Аудит функційної безпеки інформаційно-комп'ютерних систем** 1. Проведення аудиту. 2. Методики аудиту. 3. Стандарти аудиту. Літ.: [14] с.210-230 [15] с.180-200 [16] с.130-150	2
17	**Моделі та методи забезпечення безпеки інформаційно-комп'ютерних систем** 1. Моделі безпеки. 2. Методи захисту інформаційних систем. Літ.: [17] с.220-240 [18] с.200-220 [20] с.100-120	2
18	**Актуальні проблеми функційної безпеки та тенденції розвитку** 1. Сучасні виклики. 2. Майбутні тенденції у функційній безпеці. Літ.: [19] с.250-270 [20] с.220-240 [21] с.190-210	2
	Разом за семестр:	**36**

Перелік лабораторних робіт

№ п/п	Теми лабораторних робіт	Кількість годин
1	Надійність невідновлюванихелементів Літ.: [4] с.20-38,127-144	4
2	Надійність відновлювалних систем Літ.: [1]	4
3	Розрахунок показників надійності систем при основному з'єднанні елементів Літ.: [2] с.373-378 [3] с.240-256	4
4	Надійність невідновлювальних резервованих систем Літ.: [17]	4
5	Надійність відновлювальних резервованих систем Літ.: [8] [11]	4
6	Підвищення надійності мережі зберігання даних інформаційних систем Літ.: [8] [19]	4
7	Визначення надійності програмного забезпечення на етапі проєктування Літ.: [8] [22]	4
8	Визначення надійності програмного забезпечення за результатами тестування та випробовувань. Літ.: [4]с.75-84 [20]	4
9	Підсумкове заняття.	2
	Разом за семестр:	**36**

Зміст самостійної (індивідуальної) роботи

Об’єм самостійної роботи з дисципліни “Операційні системи та технології їх захисту” становить 78 годин. Він включає опрацювання теоретичного матеріалу (лекційного, методичних вказівок та літературних джерел), підготовку до тестування, виконання практичних завдань, підготовку до виконання та захисту лабораторних робіт. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

Номер тижня	Теми самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу лекції №1. Підготовка до виконання лабораторної роботи №1.	3
2	Опрацювання теоретичного матеріалу лекції №2. Підготовка до виконання лабораторної роботи №1.	4
3	Опрацювання теоретичного матеріалу лекції №3. Підготовка до виконання лабораторної роботи №2. Підготовка до захисту лабораторної роботи №1.	2
4	Опрацювання теоретичного матеріалу лекції №4. Підготовка до виконання лабораторної роботи №2. Підготовка до захисту лабораторної роботи №1.	3
5	Опрацювання теоретичного матеріалу лекції №5. Підготовка до виконання лабораторної роботи №3. Підготовка до захисту лабораторної роботи №2.	2
6	Опрацювання теоретичного матеріалу лекції №6. Підготовка до виконання лабораторної роботи №3. Підготовка до захисту лабораторної роботи №2.	1
7	Опрацювання теоретичного матеріалу лекції №7. Підготовка до виконання лабораторної роботи №4. Підготовка до захисту лабораторної роботи №3.	3
8	Опрацювання теоретичного матеріалу лекції №8. Підготовка до виконання лабораторної роботи №4. Підготовка до захисту лабораторної роботи №3.	3
9	Опрацювання теоретичного матеріалу лекції №9. Підготовка до виконання лабораторної роботи №5. Підготовка до захисту лабораторної роботи №4.	3
10	Опрацювання теоретичного матеріалу лекції №10. Підготовка до виконання лабораторної роботи №5. Підготовка до захисту лабораторної роботи №4.	2
11	Опрацювання теоретичного матеріалу лекції №11. Підготовка до виконання лабораторної роботи №6. Підготовка до захисту лабораторної роботи №5.	3
12	Опрацювання теоретичного матеріалу лекції №12. Підготовка до виконання лабораторної роботи №6. Підготовка до захисту лабораторної роботи №5.	3
13	Опрацювання теоретичного матеріалу лекції №13. Підготовка до виконання лабораторної роботи №7. Підготовка до захисту лабораторної роботи №6.	3
14	Опрацювання теоретичного матеріалу лекції №14. Підготовка до виконання лабораторної роботи №7. Підготовка до захисту лабораторної роботи №6.	2
15	Опрацювання теоретичного матеріалу лекції №15. Підготовка до виконання лабораторної роботи №8. Підготовка до захисту лабораторної роботи №7.	3
16	Опрацювання теоретичного матеріалу лекції №16. Підготовка до виконання лабораторної роботи №8. Підготовка до захисту лабораторної роботи №7.	2
17	Опрацювання теоретичного матеріалу лекції №17. Підготовка до захисту лабораторної роботи №8. Підготовка до тестування.	3
18	Опрацювання теоретичного матеріалу лекції №18. Підготовка до захисту лабораторної роботи №8. Підготовка до тестування.	3
	Разом за семестр:	**48**

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції пояснювально-ілюстративними та проблемними методами з супроводом презентаційних матеріалів, лабораторні роботи проводяться з використанням практичних, продуктивних, проблемних та контекстних методів, із застосуванням методів моделювання та сучасних інформаційно-комп‘ютерних технологій і мають за мету – набуття студентами практичних навичок оцінки ризиків, управління інцидентами інформаційної та/або кібербезпеки, використання сучасних програмних систем оцінки ризиків та управління інформаційною безпекою, використання сучасних інформаційних технологій, пов‘язаних з захистом інформації. Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: обговорення проблемних питань під час лекцій, прилюдні захисти лабораторних робіт з обґрунтуванням прийнятих рішень щодо вибору методів рішення завдань в діалозі з викладачем і групою сприяють формуванню і удосконаленню вмінь публічних виступів, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики; адаптованість, вміння користуватися інтернет-ресурсами та іншими джерелами інформації, синтезувати та критично осмислювати інформацію з різних джерел передбачені специфікою дисципліни; обмежений час на виконання лабораторних робіт і контрольних завдань, чітко визначені і надані в силабусі терміни проходження контрольних точок і відпрацювання заборгованостей сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту). При вивченні дисципліни можуть бути зараховані результати навчання, здобуті у неформальній освіті. Визнання результатів навчання, здобутих у неформальній освіті, реалізується згідно з чинним законодавством і регулюється Положенням про порядок визнання та перезарахування результатів навчання здобувачів вищої освіти у ХНУ

МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни.

При цьому використовуються такі методи поточного контролю:

- захист лабораторних робіт;
- захист практичних робіт.

Семестровий контроль проводиться у формі заліку. При виведенні підсумкової семестрової оцінки враховуються результати поточного контролю (залік за рейтингом формується автоматично за результатами поточного контролю).

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами

	Аудиторна робота		**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Практичні заняття	Залік за рейтингом
Тема	1-4	1-4	
Ваговий коефіцієнт	0,8	0,1	

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторне заняття, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторне заняття викладач оголошує одразу після захисту звіту з лабораторної роботи і проставляє в електронний журнал дисципліни.

Оцінювання практичних занять. Оцінка, яка виставляється за практичне заняття, складається з таких елементів: здатність обрати оптимальний спосіб рішення завдання і обґрунтувати зроблений вибір; правильність та самостійність розв'язування задач, якість отримуваних результатів; вільне володіння студентом спеціальною термінологією і застосовуваними методами дисципліни; уміння фахово обґрунтувати прийняті конструктивні та аналітичні рішення. Оцінку, отриману на практичному занятті, викладач оголошує студенту одразу після його відповіді і проставляє в електронний журнал дисципліни. Впродовж семестру студент має отримати на практичних заняттях щонайменше три позитивні оцінки, щоб виконати програму дисципліни.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	**Узагальнений критерій**
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні

	запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов’язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка «задовільно».

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Залік вважається зданим при отриманні студентом за зведеними результатами поточного контролю підсумкової оцінки з дисципліни від 3,00 до 5,00 балів. При цьому за вітчизняною шкалою ставиться оцінка за двобальною шкалою, а за шкалою ECTS – оцінка, що відповідає набраній студентом кількості балів.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Інституційна інтервальна шкала балів**	**Інституційна оцінка, критерії оцінювання**		
A	4,75–5,00	5	Зараховано	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4		***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4		***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3		***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3		***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	Незараховано	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2		***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ
ЗДОБУТИХ СТУДЕНТАМИ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Що таке функційна безпека ІКС, і які основні причини її важливості?
2. Які фактори впливають на функційну безпеку ІКС?
3. Які основні характеристики ІКС визначають їхню функційну безпеку згідно з міжнародними стандартами?
4. Як розрізняються справний, несправний, працездатний та граничний стани ІКС у контексті функційної безпеки?
5. Які основні види відмов ІКС і як вони класифікуються з точки зору функційної безпеки?
6. Які основні елементи складають теорію функційної безпеки ІКС?
7. Як теорія ймовірності використовується для дослідження функційної безпеки ІКС?
8. Що таке функція розподілу ймовірностей, і як вона використовується в контексті функційної безпеки ІКС?
9. Які основні правила обчислення ймовірностей подій, що впливають на функційну безпеку?
10. Як визначається ймовірність безвідмовної роботи ІКС з точки зору функційної безпеки?
11. Які основні фактори впливають на функційну безпеку ІКС?
12. Як умови експлуатації впливають на функційну безпеку ІКС?
13. Які види відмов найбільш характерні для компонентів ІКС з точки зору функційної безпеки?
14. Як враховується людський фактор та його вплив на функційну безпеку ІКС?
15. Які основні заходи можуть бути застосовані для підвищення функційної безпеки ІКС?
16. Що таке структурно-логічний аналіз і як він використовується для забезпечення функційної безпеки ІКС?
17. Які основні етапи проведення структурно-логічного аналізу ІКС?
18. Як визначаються критичні вузли та їх вплив на загальну функційну безпеку системи?
19. Що таке структурна схема надійності та як її побудувати у контексті функційної безпеки?
20. Які методи використовуються для аналізу відмов ІКС з точки зору функційної безпеки?
21. Що таке резервування і які його основні типи у контексті функційної безпеки ІКС?
22. Які основні принципи резервування ІКС для забезпечення функційної безпеки?
23. Як резервування впливає на показники функційної безпеки ІКС?
24. Які методи застосовуються для розрахунку функційної безпеки систем з резервуванням?
25. Які переваги та недоліки має використання резервування у ІКС для забезпечення функційної безпеки?
26. Як визначається ймовірність безвідмовної роботи систем з резервуванням у контексті функційної безпеки?
27. Які методи використовуються для розрахунку функційної безпеки резервованих систем?
28. Як кількість резервних елементів впливає на загальну функційну безпеку системи?
29. Які математичні моделі застосовуються для аналізу функційної безпеки резервованих систем?
30. Які особливості має розрахунок функційної безпеки для паралельного та послідовного резервування?

31. Які основні методи випробувань на функційну безпеку технічних систем?
32. Як проводяться випробування на функційну безпеку в умовах реальної експлуатації?
33. Які параметри вимірюються під час випробувань на функційну безпеку?
34. Як інтерпретуються результати випробувань на функційну безпеку?
35. Які переваги та недоліки мають різні методи випробувань на функційну безпеку?
36. Які фактори впливають на функційну безпеку комп’ютерних мереж?
37. Як оцінюється функційна безпека комп’ютерної мережі?
38. Які методи підвищення функційної безпеки використовуються в комп’ютерних мережах?
39. Як впливає архітектура мережі на її функційну безпеку?
40. Які основні виклики пов'язані з забезпеченням функційної безпеки в комп’ютерних мережах?
41. Що таке функційна безпека програмного забезпечення і які основні чинники на неї впливають?

42. Як оцінюється функційна безпека програмного забезпечення?
43. Які методи забезпечення функційної безпеки використовуються при розробці ПЗ?
44. Які основні показники функційної безпеки програмного забезпечення?
45. Як впливають тестування та верифікація на функційну безпеку програмного забезпечення?
46. Які основні математичні моделі використовуються для оцінки функційної безпеки програмних комплексів?
47. Як моделюється функційна безпека складних програмних систем?
48. Які показники враховуються в математичних моделях функційної безпеки ПЗ?
49. Як оцінюється ефективність методів підвищення функційної безпеки ПЗ?
50. Які переваги та недоліки мають різні математичні моделі функційної безпеки ПЗ?
51. Які основні показники функційної безпеки програмного забезпечення?
52. Як визначаються ймовірність безвідмовної роботи та середній час до відмови для ПЗ у контексті функційної безпеки?
53. Які математичні моделі використовуються для аналізу функційної безпеки ПЗ?
54. Як впливає архітектура програмного забезпечення на його функційну безпеку?
55. Які методи використовуються для прогнозування функційної безпеки ПЗ?
56. Які методи використовуються для контролю арифметичних операцій у контексті функційної безпеки?
57. Як проводиться діагностика комбінаційних схем з точки зору функційної безпекі?
58. Які типи помилок найбільш характерні для арифметичних операцій у контексті функційної безпекі?
59. Як визначаються показники функційної безпекі для комбінаційних схем?
60. Які методи застосовуються для підвищення функційної безпеки арифметичних операцій та комбінаційних схем?
61. Що таке діагностування і для чого воно використовується в ІКС з точки зору функційної безпеки?
62. Які основні методи діагностування існують для забезпечення функційної безпеки?
63. Як проводиться діагностування комп'ютерних систем у контексті функційної безпеки?
64. Які параметри враховуються при діагностуванні ІКС з точки зору функційної безпеки?
65. Які показники ефективності діагностування використовуються у контекст?
66. Які основні методи побудови тестів для комбінаційних схем у контексті функційної безпеки?
67. Як визначаються критерії ефективності тестів для комбінаційних схем з точки зору функційної безпеки?
68. Які типи тестів використовуються для діагностування комбінаційних схем з точки зору функційної безпеки?
69. Як проводиться верифікація та валідація тестів для комбінаційних схем у контексті функційної безпеки?
70. Які основні проблеми виникають при тестуванні комбінаційних схем з точки зору функційної безпеки?
71. Що таке сигнатурний аналіз і для чого він використовується у контексті функційної безпеки ІКС?
72. Які основні методи сигнатурного аналізу існують для забезпечення функційної безпеки?
73. Як проводиться сигнатурний аналіз технічних систем з точки зору функційної безпеки?
74. Які показники враховуються при сигнатурному аналізі для оцінки функційної безпеки?
75. Які переваги та недоліки має сигнатурний аналіз у порівнянні з іншими методами аналізу функційної безпеки?

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни “Функційна безпека інформаційно комп’ютерних систем” повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, розміщеною в електронному варіанті в модульному середовищі.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Safety and Security of Cyber-Physical Systems by Frank J. Furrer, Oliver Goerlitz, Norbert Pohlmann. Springer, 2021. 450 p.
2. Security and Resilience in Cyber-Physical Systems by Masoud Tabib, Mahdi Zareapoor. Elsevier, 2022. 300 p.
3. Безпека інформаційно-комунікаційних систем / Грайворонський М.В., Новіков О.М. Київ: КНУ, 2021. 412 с.
4. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems by Eric D. Knapp, Joel Thomas Langill. Elsevier, 2021. 400 p.
5. Safety-I and Safety-II: The Past and Future of Safety Management by Erik Hollnagel. CRC Press, 2021. 240 p.
6. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах. Одеса: ОНУ, 2020. 350 с.
7. Захист інформації в комп'ютерних системах / І.А. Терейковський, С.О. Гнатюк. Харків: ХНУРЕ, 2020. 300 с.
8. Practical Industrial Cybersecurity: ICS, SCADA, and IIoT by Pascal Ackerman. Packt Publishing, 2021. 450 p.
9. Cyber-Physical Systems: Foundations, Principles and Applications by Houbing Song, Danda B. Rawat, Sabina Jeschke, Christian Brecher. Academic Press, 2022. 500 p.
10. Critical Infrastructure Protection: Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense by Javier Lopez, Roberto Setola, Stephen D. Wolthusen. Springer, 2021. 420 p.
11. Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework by Jonathan Reuvid. Routledge, 2022. 300 p.
12. Risk Management Framework: A Lab-Based Approach to Securing Information Systems by James Broad, James W. Graves. Syngress, 2021. 350 p.

13. Додаткова

14. Оцінка ризиків в інформаційних системах / О.В. Гайдай, Ю.М. Гончарова. Дніпро: ДНУ, 2021. 275 с.
15. Cybersecurity Audit: Developing a Successful Program by Douglas J. Landoll. Auerbach Publications, 2022. 450 p.
16. Audit and Assurance Services by Alvin A. Arens, Randal J. Elder, Mark S. Beasley. Pearson, 2021. 720 p.
17. Аудит інформаційної безпеки / П.І. Колесник, М.М. Гуменюк. Львів: Видавництво Львівської політехніки, 2022. 230 с.
18. Security Engineering: A Guide to Building Dependable Distributed Systems by Ross Anderson. Wiley, 2021. 1200 p.
19. Computer Security: Principles and Practice by William Stallings, Lawrie Brown. Pearson, 2022. 800 p.
20. Trends in Cybersecurity: Critical Infrastructure and the Next Generation of Threats by Larry Clinton. Routledge, 2022. 280 p.
21. Cybersecurity Threats, Malware Trends, and Strategies by Nicholas Antill. Syngress, 2021. 320 p.
22. Сучасні проблеми та тенденції розвитку інформаційної безпеки / В.П. Петров, І.О. Соловйов. Київ: КНУ, 2022. 240 с.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання MOODLE (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань) Доступ до ресурсу: https://msn.khnu.km.ua.
2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php.