ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету інформаційних технологій
_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
« 29 » 08 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Функційна безпека інформаційних та комп'ютерних систем
Назва дисципліни

Призначення Робочої програми	Для освітніх програм різних спеціальностей
Рівень вищої освіти*	Другий (магістерський)
Мова навчання	Українська
Обсяг дисципліни, кредитів ЄКТС	8
Статус дисципліни	Вибіркова
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма здобуття освіти	Обсяг дисципліни		Кількість годин						Форма семестрового контролю
			Аудиторні заняття					Самостійна робота (в т.ч. ІРЗ)	
	Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття		Залік
Д	8	240	66	32	34			174	+

Примітка: *Вибіркову навчальну дисципліну, яку кафедра рекомендує для певного рівня вищої освіти / спеціальності, мають право вибирати здобувачі інших рівнів та спеціальностей університету.

Робоча програма складена _____ д-р філософії, ст. викл. Микола СТЕЦЮК
Підпис Науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Схвалена на засіданні кафедри кібербезпеки

Протокол від « 29 » 08.2025 р. №1

Зав. кафедри кібербезпеки _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

2. ПОЯСНЮВАЛЬНА ЗАПИСКА

Дисципліна «Функційна безпека інформаційних та комп'ютерних систем» відноситься до циклу вибіркових дисциплін та охоплює сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних та комп'ютерних систем і технологій на об'єктах інформаційної діяльності та критичних інфраструктур; програмне та програмно-апаратне забезпечення (засоби) для забезпечення функційної безпеки; системи управління функційною безпекою; технології, методи, моделі та засоби забезпечення функційної безпеки; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків).

Мета дисципліни. Формування у студентів системних знань і практичних навичок з розробки, аналізу та забезпечення функційної безпеки інформаційних та комп'ютерних систем, методів виявлення та оцінки ризиків, застосування сучасних технологій та інструментів для створення надійних та безпечних систем.

Предмет дисципліни. Сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних та комп'ютерних систем і технологій на об'єктах інформаційної діяльності та критичних інфраструктур; програмне та програмно-апаратне забезпечення (засоби) для забезпечення функційної безпеки; системи управління функційною безпекою; технології, методи, моделі та засоби забезпечення функційної безпеки; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків).

Завдання дисципліни. Формування у майбутніх спеціалістів умінь, навичок та компетентностей для аналізу надійності та функційної безпеки типових компонентів та систем кібербезпеки, оцінювання та забезпечення показників надійності та безпеки відповідно до вимог.

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: *знати* та *розуміти* поняття функційної безпеки та її відмінність від інформаційної безпеки, роль функційної безпеки у сучасних системах. нормативні вимоги та стандарти у сфері функційної безпеки, методологію розробки безпечних систем; *виявляти* та *аналізувати* ризики та загрози функційної безпеки, небезпечні ситуації та їх наслідки, *визначати* критичні функції та компоненти системи; *розробляти* безпечну архітектуру системи, *застосовувати* надійні компоненти та технології, методи захисту від відмов та збоїв, *проводити* тестування та верифікацію безпеки; *розробляти* безпечний програмний код, *застосувати* методи статичного та динамічного аналізу коду, захист від уразливостей та помилок; *розробляти* надійні апаратні компоненти, *застосувати* захист від фізичних атак, *використовувати* відмовостійкі архітектури; вміти використовувати на практиці інструментами аналізу безпеки, *розробляти* плани забезпечення безпеки; *проводити* аудит та сертифікації систем.

3. СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	**Кількість годин відведених на:**		
	лекції	**лабораторні роботи**	**СРС**
Тема 1. Функційна безпека та надійність	8	12	42
Тема 2. Методи аналізу та підвищення функційної безпеки	8	12	42
Тема 3. Практичні аспекти функційної безпеки в ІКС	8	10	42
Тема 4. Прогнозування та управління безпекою	8	-	48
Разом:	**32**	**34**	**174**

4. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

4.1 Зміст лекційного курсу

Перелік лекцій

Номер лекції	Перелік тем лекцій, їх анотація	Години
Тема 1. Функційна безпека та надійність		**8**
1	**Питання та визначення функційної безпеки.** Визначення функційної безпеки. Мета функційної безпеки. Принципи функційної безпеки. Літ.: [[1] с.12-25 [2] с.10-30 [3] с.20-40	2
2	**Теорія надійності** Основні поняття надійності. 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** Внутрішні фактори. Зовнішні фактори. Вплив людського фактору. Літ.: [2] с.45-60 [8] с.60-75 [7] с.30-50	2
4	**Структурно-логічний аналіз технічних систем** Методи структурного аналізу. Методи логічного аналізу. Аналіз відмов. Літ.: [5] с.70-85 [4] с.90-110 [7] с.40-60	2
Тема 2. Методи аналізу та підвищення функційної безпеки		**8**
5	**Резервування як метод підвищення функційної безпеки** Типи резервування. Переваги резервування. Недоліки резервування. Літ.: [10] с.90-110 [9] с.130-150 [8] с.70-90	2
6	**Розрахунок надійності систем з резервуванням** Методи розрахунку надійності. Приклади розрахунків. Літ.: [9] с.115-130 [8] с.130-145 [6] с.50-70	2
7	**Випробування на функційну безпеку ІКС** Методи випробувань. Аналіз результатів. Літ.: [8] с.140-155 [5] с.155-175 [3] с.80-100	2
8	**Функційна безпека комп'ютерних мереж** Методи забезпечення безпеки мереж. Основні загрози. Літ.: [17] с.160-175 [19] с.175-190 [6] с.90-110	2
Тема 3. Практичні аспекти функційної безпеки в ІКС		**8**
9	**Показники функційної безпеки мереж** Основні показники. Методи вимірювання. Літ.: [19] с.180-195 [4] с.200-220 [3] с.110-130	2
10	**Функційна безпека програмного забезпечення** Методи забезпечення безпеки ПЗ. Аналіз вразливостей. Літ.: [18] с.200-215 [2] с.215-230 [7] с.150-170	2
11	**Математичні моделі надійності програмних комплексів** Статистичні моделі. Аналітичні моделі. Оцінка надійності програмного забезпечення. Літ.: Літ.: [9] с.220-235 [1] с.235-250 [7] с.170-190	2
12	**Методи оцінки функційної безпеки** Основні методи оцінки. Практичне застосування. Літ.: [1] с.240-255 [2] с.255-270 [3] с.130-150	2
Тема 4. Прогнозування та управління безпекою		**8**
13	**Прогнозування функційної безпеки** Методи прогнозування. Моделювання надійності. Літ.: [4] с.260-275 [5] с.275-290 [7] с.60-80	2
14	**Управління функційною безпекою. Оцінка ризиків функційної безпеки**	2

	Стратегії управління. Впровадження систем управління. Методи оцінки ризиків. Аналіз ризиків. Управління ризиками. Літ.: [2] с.280-295 [10] с.90-110 [3] с.180-200 [11] с.150-170 [12] с.130-150 [13] с.90-110	
15	**Аудит функційної безпеки інформаційно-комп'ютерних систем** Проведення аудиту. Методики аудиту. Стандарти аудиту. Літ.: [14] с.210-230 [15] с.180-200 [16] с.130-150	2
16	**Моделі та методи забезпечення безпеки інформаційно-комп'ютерних систем** Моделі безпеки. Методи захисту інформаційних систем. Літ.: [17] с.220-240 [18] с.200-220 [20] с.100-120	2
	Разом за семестр:	**32**

4.2 Зміст лабораторних робіт

Перелік лабораторних робіт

№ п/п	Теми лабораторних робіт	Кількість годин
Тема 1. Функційна безпека та надійність		**12**
1	Надійність невідновлювальних елементів Літ.: [4] с.20-38,127-144	4
2	Надійність відновлювальних систем Літ.: [1]	4
3	Розрахунок показників надійності систем при основному з'єднанні елементів Літ.: [2] с.373-378 [3] с.240-256	4
Тема 2. Методи аналізу та підвищення функційної безпеки		**12**
4	Підвищення надійності невідновлювальних резервованих систем Літ.: [17]	4
5	Підвищення надійності відновлювальних резервованих систем Літ.: [8] [11]	4
6	Підвищення надійності мережі зберігання даних інформаційних систем Літ.: [8] [19]	4
Тема 3. Практичні аспекти функційної безпеки в ІКС		**10**
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	Узагальнення матеріалу. Тестування	2
	Разом за семестр:	**34**

4.3 Зміст самостійної (у т.ч. індивідуальної) роботи

Самостійна робота студентів полягає у опрацюванні теоретичного матеріалу з відповідних джерел інформації, підготовці до виконання та захисту лабораторних робіт, до тестування тощо. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

№ тижня	Теми самостійної роботи (І семестр)	Кількість годин
1	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №1. Підготовка до виконання лабораторної роботи №1.	10
2	Опрацювання теоретичного матеріалу лекції №2. Оформлення звіту та підготовка до захисту лабораторної роботи №1.	11

3	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №3. Підготовка до виконання лабораторної роботи №2.	10
4	Опрацювання теоретичного матеріалу лекції №4. Оформлення звіту та підготовка до захисту лабораторної роботи №2.	11
5	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №5. Підготовка до виконання лабораторної роботи №3.	10
6	Опрацювання теоретичного матеріалу лекції №6. Оформлення звіту та підготовка до захисту лабораторної роботи №3.	11
7	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №7. Підготовка до виконання лабораторної роботи №4.	10
8	Опрацювання теоретичного матеріалу лекції №8. Оформлення звіту та підготовка до захисту лабораторної роботи №4.	11
9	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №9. Підготовка до виконання лабораторної роботи №5.	10
10	Опрацювання теоретичного матеріалу лекції №10. Оформлення звіту та підготовка до захисту лабораторної роботи №5.	11
11	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №11. Підготовка до виконання лабораторної роботи №6.	10
12	Опрацювання теоретичного матеріалу лекції №12. Оформлення звіту та підготовка до захисту лабораторної роботи №6.	11
13	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №13. Підготовка до виконання лабораторної роботи №7.	10
14	Опрацювання теоретичного матеріалу лекції №14. Оформлення звіту та підготовка до захисту лабораторної роботи №7.	11
15	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №15. Підготовка до виконання лабораторної роботи №8.	10
16	Опрацювання теоретичного матеріалу лекції №16. Оформлення звіту та підготовка до захисту лабораторної роботи №8.	11
17	Підготовка до тестування за пройденим теоретичним матеріалом.	6
	Разом за семестр:	**174**

5. ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться з використанням словесних, наочних та проблемних методів з супроводом презентаційних матеріалів; лабораторні роботи – з використанням практичних та частково-пошукових методів, із застосуванням сучасних інформаційно-комп'ютерних технологій; самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання та захисту лабораторних робіт, тестування), з використанням пояснювально-ілюстративних та дослідницьких методів, інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

6. МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочою програмою і графіком освітнього процесу, в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

- оцінювання результатів захисту лабораторних робіт;
- тестовий контроль теоретичного матеріалу;

Підсумкова семестрова оцінка виставляється за результатами поточного контролю. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, вважається таким, який ***має*** академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період

екзаменаційної сесії або за графіком, встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

7. ПОЛІТИКА ДИСЦИПЛІНИ

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, що передбачені чинними положеннями Університету про організацію і навчально-методичне забезпечення освітнього процесу. Зокрема, проходження інструктажу з техніки безпеки; відвідування занять з дисципліни є обов'язковим. За об'єктивних причин (підтверджених документально) теоретичне навчання за погодженням із лектором може відбуватись в он-лайн режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до лабораторних занять (вивчення теоретичного матеріалу з теми, попередню підготовку протоколу роботи, активно працювати на занятті, якісно підготувати звіт (відповідно до теми роботи), захистити результати виконаної роботи, брати участь у дискусіях щодо прийнятих конструктивних рішень при виконанні здобувачами лабораторних робіт тощо).

Здобувачі вищої освіти зобов'язані дотримуватися термінів виконання усіх видів робіт у встановлені терміни, передбачених робочою програмою навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо здобувач захистив її на наступному після виконання роботи занятті. Пропущене лабораторне заняття здобувач зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння здобувачем теоретичного матеріалу з дисципліни оцінюється за результатами тестування.

Здобувач вищої освіти, виконуючи лабораторні роботи, тестування з дисципліни з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення плагіату в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності ***не допускаються.***

У межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах (за наявності такого переліку, доцільно вказати рекомендовані курси), які сприяють формування компетентностей і поглибленню результатів навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

8. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗДОБУВАЧІВ ОСВІТИ

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Залежно від важливості окремих видів навчальної роботи, і їх ролі у формуванні компетентностей і результатів навчання, визначених освітньою програмою, розробники Робочої програми присвоюють кожному виду навчальної роботи (структурній одиниці) з дисципліни певну кількість балів. При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє йому певну кількість балів із встановлених Робочою програмою для цього виду роботи. При цьому кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

Будь-які форми порушення академічної доброчесності ***не допускаються***.

При оцінюванні результатів навчання здобувачів вищої освіти з будь-якого виду навчальної роботи (структурної одиниці) рекомендується використовувати наведені нижче узагальнені критерії:

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	**Узагальнений зміст критерія оцінювання**
Відмінно (високий)	Здобувач вищої освіти 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 мовою викладання (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними приладами та інструментами, прикладними програмами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–три несуттєві ***похибки***.
Добре (середній)	Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, 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 правил, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–три ***несуттєві помилки***.
Задовільно (достатній)	Здобувач вищої освіти 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 здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, 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 (недостатній)	Здобувач вищої освіти 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 здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни.

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання здобувачів

Аудиторна робота								**Контрольні заходи**	**Семестровий контроль**
Лабораторні роботи №:								Тестовий контроль:	Залік
1	2	3	4	5	6	7	8	Т 1-4	
Кількість балів за вид навчальної роботи (мінімум-максимум)									
6-10	6-10	6-10	6-10	6-10	6-10	6-10	6-10	12-20	За рейтингом
48-80								**12-20**	**60-100***

Примітки: Т – тема навчальної дисципліни;

*За набрану з будь-якого виду роботи (дисципліни) кількість балів нижче встановленого мінімуму здобувач отримує незадовільну оцінку і має її перездати у встановлений викладачем (деканом) термін. Інституційна оцінка встановлюється відповідно до таблиці «**Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС**».

Оцінювання результатів захисту лабораторної роботи

Виконана й оформлена відповідно до встановлених Методичними рекомендаціями вимог лабораторна робота комплексно оцінюється викладачем при її захисті з урахуванням таких критеріїв: самостійність та правильність виконання; якість оформлення звіту; вільне володіння

здобувачем спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти та рівня досягнення здобувачем запланованих ПРН та сформованих компетентностей з присвоєнням йому відповідної суми балів.

У випадку виявлення здобувачем рівня знань, нижчого ніж 60 відсотків від максимального балу, встановленого Робочою програмою для кожної структурної одиниці, лабораторна робота йому ***не зараховується*** і для її захисту він має детальніше опрацювати матеріал з теми роботи, методику її виконання, виправити грубі помилки та повторно вийти на її захист у призначений для цього викладачем час.

Оцінювання результатів навчання з теоретичного матеріалу

Тест, передбачений Робочою програмою, складається із 20 тестових завдань, кожне з яких є рівнозначним. Максимальна сума балів, яку може набрати здобувач, складає 20.

Відповідно до таблиці структурування видів робіт за тематичний контроль здобувач залежно від кількості правильних відповідей може отримати від 12 до 20 балів.

Розподіл балів в залежності від наданих правильних відповідей на тестові завдання

Кількість правильних відповідей	0-11	12	13	14	15	16	17	18	19	20
Відсоток правильних відповідей	0-59	60-65		66-72	73-82		83-89	90-100		
Кількість балів	-	12	13	14	15	16	17	18	19	20

На тестування відводиться 20 хвилин. Правильні відповіді записуються у талоні відповідей. Здобувач може також пройти тестування і в он-лайн режимі у Модульному середовищі для навчання. При отриманні негативної оцінки тест слід перездати до терміну ***наступного*** контролю.

Для кожного окремого виду завдань підсумкового семестрового контролю застосовуються критерії оцінювання навчальних досягнень здобувача вищої освіти, наведені вище (**Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти)**.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Рейтингова шкала балів**	**Інституційна шкала (Опис рівня досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни**	
		Залік	**Іспит/диференційований залік**
A	90-100	Зараховано	***Відмінно*/*Excellent*** – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом
B	83-89		***Добре*/*Good*** – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом
C	73-82		
D	66-72		***Задовільно*/*Satisfactory*** – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни
E	60-65		
FX	40-59	Незараховано	***Незадовільно*/*Fail*** – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом
F	0-39		***Незадовільно*/*Fail*** – Результати навчання відсутні

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання з усіх видів робіт до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС у наведеній вище таблиці.

Семестровий залік виставляється на останньому занятті за умови якщо загальна сума балів, яку накопичив здобувач з дисципліни (іншого освітнього компонента) за результатами ***поточного*** контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «***зараховано***», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення. Присутність здобувача у цьому випадку не є обов'язковою.

9. ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ 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?

10. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі для навчання: https://msn.khmnu.edu.ua/course/view.php?id=9012.

11. МАТЕРІАЛЬНО-ТЕХНІЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Інформаційна та комп’ютерна підтримка: ПК, ноутбук, планшет, смартфон або інший мобільний пристрій, проєктор, доступ до мережі Інтернет, робота з презентаціями.

Вивчення навчальної дисципліни не потребує використання спеціального програмного прикладного забезпечення, крім загальновживаних програм і операційних систем.

12. 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

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.

13. ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=9012
2. Електронна бібліотека ХНУ. URL: http://lib.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://library.khmnu.edu.ua/

ФУНКЦІЙНА БЕЗПЕКА ІНФОРМАЦІЙНИХ ТА КОМП'ЮТЕРНИХ СИСТЕМ

Тип дисципліни	Вибіркова
Рівень вищої освіти	Другий (магістерський)
Мова викладання	Українська
Семестр	-
Кількість встановлених кредитів ЄКТС	8
Форми здобуття освіти, для яких викладається дисципліна	Очна (денна)

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: *знати* та *розуміти* поняття функційної безпеки та її відмінність від інформаційної безпеки, роль функційної безпеки у сучасних системах. нормативні вимоги та стандарти у сфері функційної безпеки, методологію розробки безпечних систем; *виявляти* та *аналізувати* ризики та загрози функційної безпеки, небезпечні ситуації та їх наслідки, *визначати* критичні функції та компоненти системи; *розробляти* безпечну архітектуру системи, *застосовувати* надійні компоненти та технології, методи захисту від відмов та збоїв, *проводити* тестування та верифікацію безпеки; *розробляти* безпечний програмний код, *застосувати* методи статичного та динамічного аналізу коду, захист від уразливостей та помилок; *розробляти* надійні апаратні компоненти, *застосувати* захист від фізичних атак, *використовувати* відмовостійкі архітектури; вміти використовувати на практиці інструментами аналізу безпеки, *розробляти* плани забезпечення безпеки; *проводити* аудит та сертифікації систем.

Зміст навчальної дисципліни. Основні вимоги до функційної безпеки комп'ютерних систем і мереж. Відмови інформаційних та комп'ютерних систем: види, причини, наслідки. Методи та моделі оцінки відмовостійкості інформаційних та комп'ютерних систем. Аналіз ризиків та планування заходів з підвищення відмовостійкості та живучості систем. Заходи з підвищення відмовостійкості та живучості інформаційних та комп'ютерних систем: резервування, дублювання, паралельна робота, моніторинг тощо. Методи та засоби діагностики та усунення відмов. Моніторинг та контроль відмовостійкості інформаційних та комп'ютерних систем. Відновлення інформаційних та комп'ютерних систем після відмов. Тестування інформаційних та комп'ютерних систем на відмовостійкість та живучість. Фізична безпека комп'ютерних систем і мереж. Захист від вірусів, хакерських атак та інших загроз. Нормативна база функційної безпеки інформаційних та комп'ютерних систем.

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для другого (магістерського) рівня вищої освіти за денною формою здобуття освіти становить 8 годин на 1 кредит ЄКТС.

Форми (методи) навчання: лекції (з використанням словесних, наочних та проблемних методів з супроводом презентаційних матеріалів); лабораторні роботи (з використанням практичних та частково-пошукових методів, із застосуванням сучасних інформаційно-комп'ютерних технологій); самостійна робота (з використанням пояснювально-ілюстративних та дослідницьких методів).

Форми оцінювання результатів навчання: оцінювання результатів захисту лабораторних робіт; тестовий контроль теоретичного матеріалу.

Вид семестрового контролю: залік.

Навчальні ресурси:

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. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/view.php?id=9012
7. Електронна бібліотека ХНУ. Доступ до ресурсу: http://lib.khmnu.edu.ua

Викладач: д-р філософії, ст. викл. Стецюк М.В.