ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

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

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології та системи захисту інформації

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	5 кредитів ЄКТС
Шифр дисципліни	ОПП.02
Мова навчання	Українська
Статус дисципліни	Обов'язкова, дисципліна професійної підготовки
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)	1	2	5	150	54	18	36			96				+

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації»

Робоча програма складена _____ канд. техн. наук, доц. Віктор ЧЕШУН
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

ТЕХНОЛОГІЇ ТА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Другий (магістерський)
Мова викладання	Українська
Семестр	Другий
Кількість встановлених кредитів ЄКТС	5
Форми навчання, для яких викладається дисципліна	Денна

Результати навчання. Студент, який успішно завершив вивчення дисципліни, повинен: *провадити* дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного захисту інформації у кіберпросторі; *досліджувати*, *розробляти* і *супроводжувати* системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури; *аналізувати, контролювати* та *забезпечувати* ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації; *досліджувати, розробляти, впроваджувати* та *використовувати* методи та засоби технічного захисту інформації бізнес/операційних процесів; *планувати* навчання, а також *супроводжувати* та *контролювати* роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

Зміст навчальної дисципліни. Проєктування та розробка захищених операційних систем. Концепції та методологія безпеки мережної інфраструктури. Технології Honeypot та Deception, DLP-системи. Проєктування та розробка захищених веб-ресурсів. Аутентифікація і системи контролю та управління доступом (СКУД). Методи та засоби захисту від витоку інформації. Захист інформації на об'єктах критичної інфраструктури. Організація режиму та охорони, робота з персоналом. Сучасні підходи до побудови систем інформаційної безпеки.

Пререквізити – моніторинг та менеджмент інформаційної безпеки, методологія організації атак та тестування на проникнення

Кореквізити – професійна практика

Запланована навчальна діяльність: лекції – 18 год., лабораторні заняття – 36 год., самостійна робота – 96 год.; разом – 150 год.

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, тестування, підсумковий контрольний захід.

Вид семестрового контролю: іспит.

Навчальні ресурси:

1. Захищені операційні системи: Конспект лекцій/ Ю. В. Баришев, О. В. Дмитришин, В. А. Каплун. Вінниця: ВНТУ, 2018. 161 с.
2. Технології забезпечення безпеки мережевої інфраструктури/ В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. К.: КУБГ, 2019. 218 с.
3. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак. К.: Видавництво НА СБ України, 2020. 256 с.
4. Сучасні методи забезпечення надійності персоналу: навчальний посібник у схемах і таблицях/ З.Б. Живко. Львів: ЛьвДУВС, 2019. 128 с.
5. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів/ Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Київ: ДУТ ННІЗІ, 2020. 167 с.
6. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua
7. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khmnu.edu.ua

Викладач: к.т.н., доцент Чешун В.М.

ВСТУП

Дисципліна «Технології та системи захисту інформації» - складова професійної підготовки магістрів зі спеціальності «Кібербезпека та захист інформації».

Метою викладання навчальної дисципліни є формування у майбутніх спеціалістів умінь та компетенцій для розробки та проєктування захищених інформаційно-комунікаційних систем; розробки, впровадження та використання методів та засобів технічного захисту інформації; систем управління доступом до інформаційних ресурсів; для планування навчання, контролю та супроводу роботи з персоналом.

Предметом дисципліни є сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); програмне та програмно-апаратне забезпечення (засоби) кіберзахисту.

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

***компетентності*:**

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

КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

результати навчання:

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

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.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

Студент, який успішно завершив вивчення дисципліни, повинен: *провадити* дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного захисту інформації у кіберпросторі; *досліджувати*, *розробляти* і *супроводжувати* системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури; *аналізувати*, *контролювати* та *забезпечувати* ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації; *досліджувати*, *розробляти*, *впроваджувати* та *використовувати* методи та засоби технічного захисту інформації бізнес/операційних процесів; *планувати* навчання, а також *супроводжувати* та *контролювати* роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	**Кількість годин відведених на:**		
	лекції	**лабораторні роботи**	**самостійну роботу**
Тема 1. Захист операційних систем	2	4	11
Тема 2. Захист мережної інфраструктури	4	12	29
Тема 3. Захист веб-ресурсів	2	4	11
Тема 4. Програмно-технічні складові систем захисту інформації	4	16	33
Тема 5. Захист інформації на об’єктах критичної інфраструктури	2	-	4
Тема 6. Організаційно-технічні та режимні заходи захисту інформації	2	-	4
Тема 7. Комплексне забезпечення інформаційної безпеки	2	-	4
Разом:	**18**	**36**	**96**

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотація	Години
	Тема 1. Захист операційних систем	
1	**Проєктування та розробка захищених операційних систем (ОС)** 1. Принципи створення захищених ОС. 2. Розробка захищених ОС “з нуля”. 3. Побудова “довірених” версій шляхом модернізації існуючих ОС. 4. Визначення вимог до архітектури комплексу засобів захисту в залежності від задач, які виконує ОС. 5. Адміністративні заходи захисту. Літ.: [1] с. 4-156	2
	Тема 2. Захист мережної інфраструктури	
2	**Концепції та методологія безпеки мережної інфраструктури** 1. Принципи організації безпеки мережної інфраструктури. 2. Моделі управління мережними ресурсами. 3. Безпека міжмережної взаємодії. 4. Технології побудови захищених корпоративних мереж. 5. Проєктування мереж, включаючи розуміння цілей безпеки, операційних цілей та компромісів між ними. Літ.: [2] с. 8-69, 183-213; [35]	2
3	**Технології Honeypot та Deception, DLP-системи** 1. Переваги та недоліки застосування технологій Sandboxing, Honeypots, Honeynets, та Deception у мережній інфраструктурі. 2. Підвищення мережної безпеки за рахунок впровадження Honeynet- та Deception-технологій. 3. Аналіз недоліків систем DLP. DLP-системи та закон. Методи для підвищення ефективності та законності DLP-систем. 4. Особливості проєктування систем DLP. Літ.: [4] с. 163-217; [24]; [25]; [26]; [27]; [28]	2
	Тема 3. Захист веб-ресурсів	
4	**Проєктування та розробка захищених веб-ресурсів** 1. Архітектура, функціонування та механізми безпеки веб-додатків і веб-серверів. 2. Взаємодія між веб-сервісами. REST-інтерфейс та його безпека. 3. Особливості застосування баз даних для побудови захищених веб-рішень 4. Відкритий проект по забезпеченню безпеки веб-додатків (OWASP). 5. Перспективи організації та виконання тестування рівня безпеки для певного веб-ресурсу. Літ.: [5]; [6]; [7]	2
	Тема 4. Програмно-технічні складові захисту інформації	
5	**Аутентифікація і системи контролю та управління доступом (СКУД)** 1. Аналіз існуючих підходів до вирішення задач аутентифікації 2. Біометрична аутентифікація на основі розпізнавання зображень (штучні нейронні та капсульні мережі, алгоритм розпізнавання облич Eigenface та його реалізація).	2

	3. Визначення вимог до СКУД відповідно до політики інформаційної безпеки. Обґрунтування моделі управління доступом. 4. Концепція та етапи створення СКУД. Розробка технічного завдання, проєктування, дослідна експлуатація, супровід. Літ.: [8] с. 115-140; [9] с. 7-135; [10]; [29]; [30]; [34]	
6	**Методи та засоби захисту від витоку інформації.** 1. Ідентифікація та дослідження каналів витоку інформації. 2. Організаційно-технічні заходи щодо блокування каналів витоку інформації на об'єкті. 3. Проєктування систем захисту від витоку інформації. Літ.: [11] с. 17-60; [31]; [32]	2
	Тема 5. Захист інформації на об'єктах критичної інфраструктури	
7	**Захист інформації на об'єктах критичної інфраструктури** 1. Визначення інформації, що потребує захисту на об'єктах критичної інфраструктури (ОКІ). 2. Канали витоку інформації та підстави їх утворення. 3. Засоби та комплекси виявлення прихованого підключення до інформаційних мереж (радіозакладні пристрої, приховане під'єднання до ліній зв'язку, приховані відеокамери, прихований майнінг тощо). 4. Порядок проведення обстеження і аналізу ОКІ з метою забезпечення захисту інформації. Літ.: [3] с. 23-52, 61-89; [11] с. 60-81; [13] с. 87-164; [14] с. 9-151; [15] с. 7-54	2
	Тема 6. Організаційно-технічні та режимні заходи захисту інформації	
8	**Організація режиму та охорони, робота з персоналом** 1. Робота з документами та документованою інформацією, організація розробки і використання документів та носіїв конфіденційної інформації, їх облік, виконання, повернення, зберігання і знищення. 2. Використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації. 3. Підбір та розстановка персоналу. 4. Навчання персоналу. 5. Контроль за роботою персоналу. 6. Відповідальність за порушення правил захисту інформації. Літ.: [12] с. 159-186, с. 202-214; [16] с. 95-104; [17] с. 7-121; [18] с. 55-149	2
	Тема 7. Комплексне забезпечення інформаційної безпеки	
9	**Сучасні підходи до побудови систем інформаційної безпеки (СІБ)** 1. Програми класифікації інформації організації та процедур компромісу інформації. 2. Інструменти та методи проєктування СІБ. Модель можливостей і зрілості (CMMI) при розробці СІБ. 3. Основні принципи побудови сучасних СІБ (системність, комплексність, безперервність, достатність, гнучкість, відкритість алгоритмів та механізмів, простота застосування засобів тощо). 4. Особливості розроблення та реалізації плану безпеки. Керування конфігурацією. Літ.: [19] с. 103-124, 210-250; [20] с. 500-564; [21]; [33]; [36]	2
	Разом за семестр:	**18**

Зміст лабораторних робіт

№ п/п	Теми лабораторних робіт	Кількість годин
1	Проєктування “довіреної” версії ОС за допомогою антивірусного захисту. Літ.: [22] с. 30-34	4
2	Проєктування захищеної мережі на основі технології Honeypot. Літ.: [24]; [25]; [26]	4
3	Проєктування захищеної мережі на основі технології Deception. Літ.: [24]; [25]; [26]	4
4	Проєктування та дослідження DLP-системи. Літ.: [27]; [28]	4
5	Забезпечення безпеки багатокомпонентних веб-додатків. Літ.: [5]; [6]	4
6	Проєктування системи аутентифікації на основі розпізнавання зображень Літ.: [9] с. 69-87	4
7	Проєктування системи відеомоніторингу, контролю та управління доступом Літ.: [10]; [23] с. 178-188	4
8	Проєктування систем захисту від витоку інформації акустичними каналами та через побічне електромагнітне випромінювання Літ.: [11] с. 26-60	4
9	Підсумкове заняття. Тестування	4
	Разом за семестр:	**36**

Зміст самостійної (у т.ч. індивідуальної) роботи

Об’єм самостійної роботи з дисципліни становить 96 годин. Він включає опрацювання лекційного матеріалу та літературних джерел, підготовку до контрольної роботи, підготовку до виконання та захисту лабораторних робіт. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

№ тижня	Теми самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу лекції №1.	4
2	Підготовка до виконання лабораторної роботи №1.	4
3	Опрацювання теоретичного матеріалу лекції №2.	4
4	Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2.	7
5	Опрацювання теоретичного матеріалу лекції №3.	4
6	Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3.	7
7	Опрацювання теоретичного матеріалу лекції №4.	4
8	Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4.	7
9	Опрацювання теоретичного матеріалу лекції №5.	4
10	Підготовка до захисту лабораторної роботи №4. Підготовка до виконання лабораторної роботи №5.	7
11	Опрацювання теоретичного матеріалу лекції №6.	4
12	Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6.	7
13	Опрацювання теоретичного матеріалу лекції №7.	4
14	Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7. Робота над КП відповідно до календарного плану.	7
15	Опрацювання теоретичного матеріалу лекції №8.	4
16	Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8.	7
17	Опрацювання теоретичного матеріалу лекції №9.	4
18	Підготовка до захисту лабораторної роботи №8. Підготовка до тестування.	7
	Разом за семестр:	96

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, методами моделювання та з застосуванням сучасних інформаційно-комп'ютерних технологій і мають за мету – набуття студентами практичних навичок для розробки та проєктування захищених інформаційно-комунікаційних систем; розробки, впровадження та використання методів та засобів технічного захисту інформації; систем управління доступом до інформаційних ресурсів; для планування навчання, контролю та супроводу роботи з персоналом.

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;
- тестування.

Семестровий контроль проводиться у формі іспиту. При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контрольного заходу.

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	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Тестування	Семестровий контроль (іспит)
Тема	1-4	5-7	1-7
Ваговий коефіцієнт	0,4	0,2	0,4

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторну роботу, складається з таких елементів: 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 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 лабораторну роботу викладач оголошує одразу після захисту звіту і проставляє в електронний журнал дисципліни.

Оцінювання тестових завдань. Тематичний тест для кожного студента складається з двадцяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 20.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	1–10	11–14	15–17	18–20
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 20 хвилин (для закритої форми тестів – по одній хвилині на кожне завдання). Правильні відповіді студент записує у талоні відповідей. При цьому усі графи для відповідей мають бути заповнені цифрами, що відповідають правильним, на погляд студента, відповідям. Через 20 хвилин студенти здають викладачу завдання з талонами відповідей.

Тестування студент може також пройти і в онлайн режимі в модульному середовищі для навчання MOODLE.

Оцінку за тестування викладач проставляє в електронний журнал дисципліни не пізніше ніж через десять днів після проведення заходу.

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з двох теоретичних питань і задачі. Під час іспиту за наданими відповідями і рішеннями (розв'язками) виконується оцінювання рівня засвоєння студентом матеріалу дисципліни.

Оцінка за підсумковий контрольний захід проставляється викладачем в електронний журнал дисципліни в день здачі іспиту і враховується в автоматизованому режимі при визначенні підсумкової семестрової оцінки студента з дисципліни за інституційною шкалою і шкалою ЄКТС

Засвоєння студентом матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями.

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.

Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невстигаючим.

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	***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	***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. Принципи створення захищених ОС.
2. Розробка захищених ОС “з нуля”.
3. Побудова “довірених” версій шляхом модернізації існуючих ОС.
4. Визначення вимог до архітектури комплексу засобів захисту в залежності від задач, які виконує ОС.
5. Адміністративні заходи захисту ОС.
6. Принципи організації безпеки мережної інфраструктури.
7. Моделі управління мережними ресурсами.
8. Безпека міжмережної взаємодії.
9. Технології побудови захищених корпоративних мереж.
10. Проєктування мереж, включаючи розуміння цілей безпеки, операційних цілей та компромісів між ними.
11. Переваги та недоліки застосування технологій Sandboxing у мережній інфраструктурі.
12. Переваги та недоліки застосування технологій Honeypots та Honeynets у мережній інфраструктурі.
13. Переваги та недоліки застосування технологій Deception у мережній інфраструктурі.
14. Підвищення мережної безпеки за рахунок впровадження Honeynet- та Deception-технологій.
15. Аналіз недоліків систем DLP.
16. Методи для підвищення ефективності та законності DLP-систем.
17. Особливості проєктування систем DLP.
18. Архітектура, функціонування та механізми безпеки веб-додатків і веб-серверів.
19. Взаємодія між веб-сервісами як елемент інформаційної безпеки.
20. REST-інтерфейс та його безпека.
21. Особливості застосування баз даних для побудови захищених веб-рішень
22. Відкритий проект по забезпеченню безпеки веб-додатків (OWASP).
23. Перспективи організації та виконання тестування рівня безпеки для певного веб-ресурсу.
24. Аналіз існуючих підходів до вирішення задач аутентифікації
25. Біометрична аутентифікація на основі розпізнавання зображень (штучні нейронні та капсульні мережі, алгоритм розпізнавання облич Eigenface та його реалізація).
26. Визначення вимог до СКУД відповідно до політики інформаційної безпеки. Обґрунтування моделі управління доступом.
27. Концепція та етапи створення СКУД. Розробка технічного завдання, проєктування, дослідна експлуатація, супровід.
28. Ідентифікація та дослідження каналів витоку інформації.
29. Організаційно-технічні заходи щодо блокування каналів витоку інформації на об’єкті.
30. Проєктування систем захисту від витоку інформації.
31. Визначення інформації, що потребує захисту на об’єктах критичної інфраструктури (ОКІ).
32. Канали витоку інформації на ОКІ та підстави їх утворення.
33. Засоби та комплекси виявлення прихованого підключення до інформаційних мереж.
34. Види прихованого підключення до інформаційних мереж (радіозакладні пристрої, приховане під’єднання до ліній зв’язку, приховані відеокамери, прихований майнінг тощо).
35. Порядок проведення обстеження і аналізу ОКІ з метою забезпечення захисту інформації.
36. Робота з документами та документованою інформацією.
37. Організація розробки і використання документів та носіїв конфіденційної інформації.
38. Облік документів та документованої інформації.

39. Виконання та повернення документів та документованої інформації.
40. Зберігання і знищення документів та документованої інформації.
41. Використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації.
42. Підбір та розстановка персоналу.
43. Навчання персоналу.
44. Контроль за роботою персоналу.
45. Відповідальність за порушення правил захисту інформації.
46. Програми класифікації інформації організації та процедур компромісу інформації.
47. Інструменти та методи проєктування СІБ.
48. Модель можливостей і зрілості (CMMI) при розробці СІБ.
49. Основні принципи побудови сучасних СІБ.
50. Особливості розроблення та реалізації плану безпеки. Керування конфігурацією.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Захищені операційні системи: Конспект лекцій / Ю. В. Баришев, О. В. Дмитришин, В. А. Каплун. Вінниця: ВНТУ, 2018. 161 с.
2. Технології забезпечення безпеки мережевої інфраструктури/ В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. К.: КУБГ, 2019. 218 с.
3. Основи інформаційної безпеки: навч. посібник/ В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
4. Основи кібербезпеки та кібероборони: підручник/ Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. Одеса.: ОНАЗ ім. О.С. Попова, 2019. 320 с.
5. OWASP Top 10 API Security Risks – 2023 [Електронний ресурс]. Режим доступу: https://owasp.org/API-Security/editions/2023/en/0x11-t10/
6. Web Application Security Testing v4.2 [Електронний ресурс]. Режим доступу: https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/
7. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу [Електронний ресурс]. Режим доступу: https://tzi.com.ua/downloads/2.5-010-03.pdf
8. Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. Львів, «Магнолія 2006», 2016. 256 с.
9. Біометричні технології: навч. посіб./ Р.Ю. Царьов, Т. М. Лемеха. Одеса: ОНАЗ ім. О.С. Попова, 2016. 140 с.
10. The Access Control Technologies Handbook. Prepared by Space and Naval Warfare Systems Center Atlantic, 2015. 53 p.
11. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник/ С.О. Іванченко, О.В Гавриленко, О.А Липський, А.С. Шевцов. К.: ІСЗЗІ НТУУ «КПІ», 2016. 104 с.
12. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак. К.: Видавництво НА СБ України, 2020. 256 с.
13. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналітична доповідь/ Д.Г. Бобро, С.П. Іванюта, С.І. Кондратов, О.М. Суходоля/ за заг. ред. О. М. Суходолі. К.: НІСД, 2019. 224 с.
14. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монограф./ О. П. Єрменчук. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.
15. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності. Навчальній посібник/ О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. К.:ДУТ, 2020. 126 с.
16. Основи інформаційної безпеки. Конспект лекцій./ Б.А. Заплотинський. КІВіП НУ “ОЮА”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. 128 с.
17. Сучасні методи забезпечення надійності персоналу: навчальний посібник у схемах і таблицях/ З.Б. Живко. Львів: ЛьвДУВС, 2019. 128 с.
18. Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. Київ: Видавничий дім «Гельветика», 2017. 168 с.
19. Проєктування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів: Видавництво Львівської політехніки, 2020. 320 с.

20. Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів: Видавництво Львівської політехніки, 2019. 580 с.
21. CMMI High Maturity Handbook [Електронний ресурс]. Режим доступу: http://uploads.worldlibrary.net/uploads/pdf/20151101020335cmmi_high_maturity_hand_book_amazon.pdf
22. Learning Malware Analysis. Explore the concepts, tools, and techniques to analyze and investigate Windows malware Security/ Edited by Monnappa K A. Packt Publishing Ltd, 2018. 500 p.
23. Проєктування та монтаж локальних комп'ютерних мереж: [навчальний посібник]/ І. М. Журавська. Миколаїв: Видавництво ЧДУ ім. Петра Могили, 2016. 396 с.

Додаткова

24. A novel honeypot based security approach for real-time intrusion detection and prevention systems/ Muhammet Baykara, Resul Das. - Journal of Information Security and Applications, Volume 41, August 2018. – pp. 103-116. - https://doi.org/10.1016/j.jisa.2018.06.004
25. Human vs bots: Detecting human attacks in a honeypot environment/ Shreya Udhani, Alexander Withers, Masooda Bashir. - 7th International Symposium on Digital Forensics and Security, ISDFS 2019. - https://doi.org/10.1109/ISDFS.2019.8757534
26. Secure and Resilient Artificial Intelligence of Things: a HoneyNet Approach for Threat Detection and Situational Awareness/ Liang Tan, Keping Yu, Fangpeng Ming, Xiaofeng Chen, Gautam Srivastava. - IEEE Consumer Electronics Magazine, 2021. – 10.1109/MCE.2021.3081874
27. Data Leakage Prevention System: A Systematic Report/ Sheela Gowr. P, Kumar. N. - International Journal of Recent Technology and Engineering (IJRTE), Volume-8 Issue-4, November 2019. – pp. 367-377. - DOI:10.35940/ijrte.D6904.118419
28. A survey on data leakage prevention systems/ Sultan Alneyadi, Elankayer Sithirasenan, Vallipuram Muthukkumarasamy. - Journal of Network and Computer Applications, Volume 62 Issue, C February, 2016. – pp. 137–152. - https://doi.org/10.1016/j.jnca.2016.01.008
29. One-Time-Username: A Threshold-based Authentication System/ Abdulrahman Alhothailya, Arwa Alrawaisa, Chunqiang Hua, Wei Li. - Procedia Computer Science 129 (2018), Elsevier Ltd. – pp. 427-431. - https://doi.org/10.1016/j.procs.2018.03.019
30. Design and Implementation of a Computerized User Authentication System for E-Learning/ Z. Faizal Khan, Sultan Refa Alotaibi. - iJET – Vol. 15, No. 9, 2020 - pp. 4-18. - https://doi.org/10.3991/ijet.v15i09.12387
31. Information leakage analysis of software: How to make it useful to IT industries?/ Kushal Anjaria, Arun Mishra/ - Faculty of Computers and Information Technology, Future University in Egypt. Production and hosting by Elsevier B.V., 2017. PP. 10-18. https://doi.org/10.1016/j.fcij.2017.04.002
32. Research on Behavior-Based Data Leakage Incidents for the Sustainable Growth of an Organization/ Jawon Kim, Jaesoo Kim, Hangbae Chang. Sustainability 2020, 12, 6217. PP. 1-14. doi:10.3390/su12156217
33. Yamfashije, Jeanne. (2017). Capability Maturity Model Integration. 10.13140/RG.2.2.35219.94247.
34. Використання розподілених хеш-таблиць надання доступу до хмарних сервісів/ Ю. П. Кльоц, І. В. Муляр, В. М. Чешун, О. В. Бурдюг// Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ: ВІКНУ, 2020. Вип. 67. С. 85–95.
35. Удосконалення систем захисту інформації в комп'ютерних мережах Державної прикордонної служби України/ Андрощук О., Коваленко О., Тітова В., Чешун В., Поляков А. Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки, 85(2-3). 2021. С. 5-21.

36. Використання інформаційних технологій для підвищення якості роботи та безпеки телекомунікаційних мереж/ Хмельницький, Ю., Чешун, В., Джулій А., Чорненький, В.// Measuring and Computing Devices in Technological Processes, (2022). (1), С. 36–42. https://doi.org/10.31891/2219-9365-2022-69-1-5

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/
2. Електронна бібліотека університету. URL: http://lib.khmnu.edu.ua/