ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету інформаційних технологій
_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
«_29_» _____08_____ 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека програм та даних

Галузь знань	F Інформаційні технології
Спеціальність	F2 Інженерія програмного забезпечення
Рівень вищої освіти	Перший (бакалаврський)
Освітньо-професійна програма	Інженерія програмного забезпечення
Обсяг дисципліни	5 кредитів ЄКТС
Шифр дисципліни	ОПП.06
Мова навчання	Українська, англійська
Статус дисципліни	Обов'язкова (фахової підготовки)
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма здобуття освіти	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття									
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття	Самостійна робота, у т.ч. ІРЗ			Залік	Іспит
Д	4	7	5	150	66	32	34			84				+

Робоча програма складена на основі освітньо-професійної програми «Інженерія програмного забезпечення» за спеціальністю F2 «Інженерія програмного забезпечення»

Програма складена _____ канд. техн. наук, доц. Віра ТІТОВА
Підпис Науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Схвалена на засіданні кафедри кібербезпеки
Протокол від «_29_»_08_.2025 №_1_

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

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

2. ЛИСТ ПОГОДЖЕННЯ

Посада	Назва факультету	Підпис	Ініціали, прізвище
Завідувач кафедри інженерії програмного забезпечення, доктор, фіз.-мат. наук, проф.	Факультет інформаційних технологій		Леонід БЕДРАТЮК
Гарант освітньо-професійної програми, доктор, фіз.-мат. наук, проф.	Факультет інформаційних технологій		Леонід БЕДРАТЮК

3. ПОЯСНЮВАЛЬНА ЗАПИСКА

Дисципліна «Безпека програм та даних» - складова професійної підготовки бакалаврів зі спеціальності «Інженерія програмного забезпечення».

Пререквізити – архітектура та проєктування ПЗ.

Постреквізити – професійна практика.

Відповідно до освітньої програми дисципліна сприяє забезпеченню наступних **компетентностей** (ІК, ФК06, ФК12) та **програмних результатів навчання** (ПРН01, ПРН04, ПРН18, ПРН21).

Мета дисципліни. Надання глибоких та міцних знань з питань захисту ПЗ від несанкціонованого копіювання програмними та програмно-апаратними методами.

Предмет дисципліни. Методи та засоби забезпечення захисту програмного забезпечення; методи і засоби підтримки цілісності, загальної функціональності і надійності програмного забезпечення.

Завдання дисципліни. Формування у майбутніх спеціалістів знань про методи імітаційного моделювання, умінь та компетенцій для забезпечення захисту програм та даних.

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: *застосовувати* інформаційні технології обробки, зберігання та передачі даних, а також методи та засоби забезпечення інформаційної безпеки ПЗ; *аналізувати*, *вибирати* і *застосовувати* сучасні досягнення науки і техніки для забезпечення інформаційної безпеки ПЗ; *використовувати* операційні системи, мережеві технології, засоби розробки інтерфейсу при конструюванні та захисті ПЗ.

4. СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин відведених на:		
	лекції	**лабораторні роботи**	**самостійну роботу**
Тема 1. Технології захисту програм та даних	14	24	48
Тема 2. Методи захисту ПЗ від несанкціонованого копіювання	18	10	36
Разом:	**32**	**34**	**84**

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1 Зміст лекційного курсу

Перелік лекцій

Номер лекції	Перелік тем лекцій, їх анотація	Години
Тема 1. Технології захисту програм та даних		**14**
1	**Введення в безпеку програм та даних**	2

	Проблеми захисту інформації в програмних системах. Критерії оцінки захищеності інформації. Види кіберзлочинів з точки зору безпеки програм та даних. Поняття і класифікація комп'ютерних вірусів. Засоби зламу програмного забезпечення. Їх класифікація. Інструментарій виявлення вразливостей в програмному коді. Літ.: [2] с. 53-89	
2	**Засоби захисту програм та даних** Автентифікація, авторизація та адміністрування дій користувачів. Засоби захисту вмісту файлів та папок. Засоби захисту вмісту локальних дисків. Антивіруси. Міжмережні екрани (брандмауери). Літ.: [1], с. 13-21, 55-71; [2] с. 53-89, 106-115	2
3	**Криптографічний захист програм та даних (частина 1)** Класичні методи шифрування. Шифр Цезаря. Квадрат Полібія. Шифр Вернама. Шифр гамування. Потокові криптосистеми. Літ.: [3], с. 6-26	2
4	**Криптографічний захист програм та даних (частина 2)** Блокова криптосистема DES. Режими шифрування. Стандарт шифрування Rijndael. Літ.: [3], с. 33-66	2
5	**Криптографічний захист програм та даних (частина 3)** Схема Діффі – Хелмана розповсюдження ключів по відкритим каналам. Криптосистема з відкритим ключем RSA. Літ.: [3], с. 76-86	2
6	**Криптографічний захист програм та даних (частина 4)** Хеш-функції. Основні алгоритми хешування. Електронний цифровий підпис. Цифровий підпис RSA. Літ.: [3], с. 86-105	2
7	**Перевірка цілісності програм і даних** Основні підходи. Перевірка цілісності за допомогою CRC-кодів. Літ.: [4], с. 231-247	2
Тема 2. Методи захисту ПЗ від несанкціонованого копіювання (НСК)		**18**
8	**Моделі розповсюдження програмного забезпечення** Безкоштовне програмне забезпечення (Freeware). Умовно безкоштовне програмне забезпечення (Demoware, Trialware, Nagware та ін.). Комерційне програмне забезпечення. Літ.: [5], с. 20-30, 47-48	2
9	**Пакувальники і їх відмінності від архіваторів** Огляд сучасних пакувальників. Ідентифікація параметрів пакування виконуваного файлу. Літ.: [5], с. 7-20	2
10	**Основні поняття ОС, необхідні для захисту програмного забезпечення** Склад та функції операційної системи. BIOS - Базова система введення-виведення. UEFI – інтерфейс розширюваної прошивки. CMOS - Complementary Metal Oxide Semiconductor. Переривання, їх роль та процедура звернення в програмах. Літ.: [5], с. 49-53	2
11	**Програмно-апаратні методи захисту ПЗ від НСК** Реєстраційні коди. Навісні захисти (протектори). Апаратні ключі. Їх будова та класифікація. Захист програм за допомогою ключа. Огляд та характеристика відомих ключів захисту. Система «SecretKey». Двухфакторна автентифікація на основі технології RSA SecurID. Літ.: [5], с. 53-64, 78-93, 108-117	2
12	**Захист програм від несанкціонованого дослідження** Основні методи та засоби дослідження програм. Способи впровадження захисних механізмів в ПЗ. Структура програм, захищених від	2

	дослідження. Літ.: [6], с. 6-12	
13	**Захист від дизасембювання** Необхідність і доцільність захисту від дизасемблювання. Основні методи протидії дизасемблюванню програм. Шифрування коду. Маніпулювання з EXE-заголовком. Літ.: [6], с. 13-30	2
14	**Захист програм шляхом обфускації** Поняття обфускації та її види. Лексична обфускація. Обфускація даних. Обфускація графа потоку управління. Аналіз ефективності роботи обфускаторів. Відомі обфускатори і їх можливості. Літ.: [6], с. 30-53	2
15	**Захист від несанкціонованого налагоджування** Огляд і класифікація налагоджувачів. Захист від налагоджувачів реального режиму. Боротьба з налагоджувачами захищеного режиму. Додаткові прийоми "витонченого" програмування. Літ.: [6], с. 65-74	2
16	**Сучасні технології дампінга і захисту від нього** Порядок завантаження програми і виділення пам'яті процесу. Доступ до пам'яті та списку процесів. Отримання дампу пам'яті обраного процесу. Програми для визначення дампу і захист від них. Методи захисту від дампінгу. Літ.: [6], с. 84-97	2
	Разом за семестр:	**32**

5.2 Зміст лабораторних робіт

Перелік лабораторних робіт

№ п/п	Теми лабораторних робіт	Кількість годин
Тема 1. Технології захисту програм та даних		**24**
1	Розмежування повноважень користувачів на основі парольної автентифікації Літ.: [2] с. 53-89	4
2	Логування дій користувачів у програмних системах Літ.: [2] с. 53-89	4
3	Захист програмного забезпечення за допомогою механізму CAPTCHA Літ.: [2] с. 53-89	4
4	Захист даних за допомогою цифрового підпису Літ.: [3] с. 94-95	4
5	Захист даних за допомогою технології Blockchain Літ.: [7], с. 8-48	4
6	Перевірка цілісності файлів на основі CRC-кодів Літ.: [4], с. 231-247	4
Тема 2. Методи захисту ПЗ від несанкціонованого копіювання (НСК)		**10**
7	Розробка умовно безкоштовного програмного забезпечення Літ.: [5], с. 47-48	4
8	Захист програмного забезпечення за допомогою механізму обфускації Літ.: [6], с. 30-53	4
9	Підсумкове заняття.	2
	Разом за семестр:	**34**

5.3 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	Кількість годин
1	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №1. Підготовка до виконання лабораторної роботи №1.	5
2	Опрацювання теоретичного матеріалу лекції №2. Оформлення звіту та підготовка до захисту лабораторної роботи №1.	5
3	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №3. Підготовка до виконання лабораторної роботи №2.	5
4	Опрацювання теоретичного матеріалу лекції №4. Оформлення звіту та підготовка до захисту лабораторної роботи №2.	5
5	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №5. Підготовка до виконання лабораторної роботи №3.	5
6	Опрацювання теоретичного матеріалу лекції №6. Оформлення звіту та підготовка до захисту лабораторної роботи №3.	5
7	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №7. Підготовка до виконання лабораторної роботи №4.	5
8	Опрацювання теоретичного матеріалу лекції №8. Оформлення звіту та підготовка до захисту лабораторної роботи №4.	5
9	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №9. Підготовка до виконання лабораторної роботи №5.	5
10	Опрацювання теоретичного матеріалу лекції №10. Оформлення звіту та підготовка до захисту лабораторної роботи №5.	5
11	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №11. Підготовка до виконання лабораторної роботи №6.	5
12	Опрацювання теоретичного матеріалу лекції №12. Оформлення звіту та підготовка до захисту лабораторної роботи №6.	5
13	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №13. Підготовка до виконання лабораторної роботи №7.	5
14	Опрацювання теоретичного матеріалу лекції №14. Оформлення звіту та підготовка до захисту лабораторної роботи №7.	5
15	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №15. Підготовка до виконання лабораторної роботи №8.	5
16	Опрацювання теоретичного матеріалу лекції №16. Оформлення звіту та підготовка до захисту лабораторної роботи №8.	5
17	Підготовка до тестування за пройденим теоретичним матеріалом.	4
	Разом за семестр:	**84**

6. 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 методів, із застосуванням технологій моделювання та застосуванням сучасних інформаційно-комп'ютерних технологій; самостійна робота – з використанням пояснювально-ілюстративних та дослідницьких методів.

7. МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лабораторних, 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.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного, так і підсумкового контролів, який проводиться з усього матеріалу дисципліни за білетами, попередньо розробленими і затвердженими на засіданні кафедри. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, ***не допускається*** до семестрового контролю поки не виконає весь обсяг, передбачений Робочою програмою для цього виду роботи. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу, встановленого для кожної структурної одиниці) з усіх видів поточного контролю і не склав іспит, 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».

8. 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 самостійну роботу та захищаючи лабораторні роботи 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).

9. 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:	Іспит	Разом

1	2	3	4	5	6	7	8	Т 1-2		балів
Кількість балів за вид навчальної роботи (мінімум-максимум)										
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	12-20	24-40	**60-100**
24-40								**12-20**	**24-40**	

Примітки: Т – тема навчальної дисципліни;

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 25 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	0-14	15-16	17-18	19-20	21-22	23-25
Відсоток правильних відповідей	0-59	60-65	66-72	73-82	83-89	90-100
Кількість балів	-	12	14	16	18	20

На тестування відводиться 25 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.

Оцінювання результатів підсумкового семестрового контролю (іспит)

Освітня програма передбачає підсумковий семестровий контроль з дисципліни у формі іспиту, завданням якого є системне й об’єктивне оцінювання підготовки здобувача з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами.

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів вищої освіти (40 балів для підсумкового контролю)

Види завдань	**Для кожного окремого виду завдань**		
	Мінімальний (достатній) бал (задовільно)	**Потенційні позитивні бали* (середній бал) (добре)**	**Максимальний (високий) бал (відмінно)**
Теоретичне питання № 1	6	8	10
Теоретичне питання № 2	6	8	10
Практичне завдання	12	16	20
Разом:	**24**		**40**

Примітка. **Позитивний бал за іспит, відмінний від мінімального (24 бали) та максимального (40 балів), знаходиться в межах 25-39 балів та розраховується як сума балів за усі структурні елементи (завдання) іспиту.*

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 нижче таблиці.

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав здобувач з дисципліни за результатами поточного та підсумкового контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «відмінно/добре/задовільно», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній здобувачем сумі балів відповідно до таблиці Співвідношення.

10. ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Проблеми захисту інформації в програмних системах.
2. Критерії оцінки захищеності інформації.
3. Види кіберзлочинів з точки зору безпеки програм та даних.
4. Поняття і класифікація комп’ютерних вірусів.
5. Засоби зламу програмного забезпечення. Їх класифікація.
6. Інструментарій виявлення вразливостей в програмному коді.
7. Автентификация, авторизація та адміністрування дій користувачів
8. Засоби захисту вмісту файлів та папок.
9. Засоби захисту вмісту локальних дисків.
10. Антивіруси.
11. Міжмережні екрани (брандмауери).
12. Шифр Цезаря.
13. Квадрат Полібія.
14. Шифр Вернама.
15. Шифр гамування.

16. Потокові криптосистеми.
17. Блокова криптосистема DES. Режими шифрування.
18. Стандарт шифрування Rijndael.
19. Схема Діффі – Хелмана розповсюдження ключів по відкритим каналам.
20. Криптосистема з відкритим ключем RSA.
21. Хеш-функції. Основні алгоритми хешування.
22. Електронний цифровий підпис. Цифровий підпис RSA.
23. Основні підходи до перевірки цілісності програм і даних.
24. Перевірка цілісності за допомогою CRC-кодів.
25. Моделі розповсюдження програмного забезпечення.
26. Безкоштовне програмне забезпечення (Freeware).
27. Умовно безкоштовне програмне забезпечення (Demoware, Trialware, Nagware та ін.).
28. Комерційне програмне забезпечення.
29. Пакувальники і їх відмінності від архіваторів
30. Огляд сучасних пакувальників.
31. Ідентифікація параметрів пакування виконуваного файлу.
32. Склад та функції операційної системи.
33. BIOS - Базова система введення-виведення.
34. UEFI – інтерфейс розширюваної прошивки.
35. CMOS - Complementary Metal Oxide Semiconductor
36. Переривання, їх роль та процедура звернення в програмах
37. Робота з дисками на фізичному рівні. Функції BIOS для роботи з дисками. Захист від НСК методом прив'язки до диску.
38. Аналіз вмісту CMOS-пам'яті для захисту від НСК.
39. Реєстраційні коди, як захист від НСК.
40. Навісні захисти (протектори).
41. Апаратні ключі. Їх будова та класифікація.
42. Захист програм за допомогою ключа.
43. Огляд та характеристика відомих ключів захисту.
44. Система «SecretKey».
45. Двухфакторна автентифікація на основі технології RSA SecurID.
46. Основні методи та засоби дослідження програм.
47. Способи впровадження захисних механізмів від несанкціонованого дослідження в ПЗ.
48. Структура програм, захищених від дослідження.
49. Необхідність і доцільність захисту від дизасемблювання.
50. Основні методи протидії дизасемблюванню програм.
51. Шифрування коду, як захист від дизасемблювання
52. Маніпулювання з EXE-заголовком, як захист від дизасемблювання.
53. Поняття обфускації та її види.
54. Лексична обфускація.
55. Обфускація даних.
56. Обфускація графа потоку управління.
57. Аналіз ефективності роботи обфускаторів.
58. Відомі обфускатори і їх можливості.
59. Огляд і класифікація налагоджувачів.
60. Захист від налагоджувачів реального режиму.
61. Боротьба з налагоджувачами захищеного режиму.
62. Додаткові прийоми “витонченого” програмування.
63. Порядок завантаження програми і виділення пам’яті процесу.
64. Доступ до пам’яті та списку процесів.
65. Отримання дампу пам’яті обраного процесу.
66. Програми для визначення дампу і захист від них.
67. Методи захисту від дампінгу.

11. 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=8776.

12. 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.

Спеціальне та прикладне програмне забезпечення: OS MS Windows 10 або вище, MS Visual Studio 2019 або вище.

13. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Безпека програм та даних: навчальний посібник/ В. І. Горбенко, А.О. Лісняк. Запоріжжя: ЗНУ, 2022. 72 с.
2. Основи інформаційної безпеки : навч. посібник/ В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
3. Основи криптології: навч. Посібник/ Н.О. Щур, О.А. Покотило. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
4. Теорія інформації і кодування: курс лекцій: навч. посіб./ А.Є.Коваленко. Київ : КПІ ім. Ігоря Сікорського, 2020. 248 с.

Додаткова

5. Захист програмного забезпечення. Частина 1: навчальний посібник/В. А. Каплун, О. В. А.В. Дудатьєв, В. П. Семеренко В.П. Вінниця: ВНТУ, 2017. 140 с.
6. Захист програмного забезпечення. Частина 2: навчальний посібник/В. А. Каплун, О. В. Дмитришин, Ю. В. Баришев. Вінниця: ВНТУ, 2017. 105 с.
7. Вступ до технології блокчейн та криптовалют. Частина 1: навчальний посібник/ Л.В.Ковальчук, А.М.Кудін, Н.В. Кучинська/ Київ: КПІ ім. Ігоря Сікорського, 2022. 141 с.
8. Четверіков І. О., Петренко А. І. Технологія Blockchain в системі захисту інформації/ Моделювання та інформ. системи в економіці: зб. наук. праць/ відп. ред. О. Є. Камінський. 2020. № 99.1. С. 162-170.
9. Корнага Я.І., Герасименко О.Ю., Базака Ю.А., Базалій М.Ю., Мухін О.В. Method of Protecting Software Code from Reengineering Using Virtual Machines. Sciences of Europe, 2020. № 58. С. 59-62.
10. Корнага Я.І., Базака Ю.А., Базалій М.Ю. Захист програмного забезпечення за допомогою заплутуючих перетворень. The scientific heritage, 2020. № 54. С. 72-75.
11. Семенов С.Г., Давидов В.В., Волошин Д.Г., Гребенюк Д.С. Метод захисту модуля програмного забезпечення на основі процедури обфускації/ Телекомунікаційні та інформаційні технології. 2019. № 4 (65). С.71-80.

14. ІНФОРМАЦІЙНІ РЕСУРСИ

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

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

Тип дисципліни	Обов'язкова
Освітній рівень	Перший (бакалаврський)
Мова викладання	Українська
Семестр	Сьомий
Кількість встановлених кредитів ЄКТС	5
Форми навчання, для яких викладається дисципліна	Очна (денна)

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: *застосовувати* інформаційні технології обробки, зберігання та передачі даних, а також методи та засоби забезпечення інформаційної безпеки ПЗ; *аналізувати*, *вибирати* і *застосовувати* сучасні досягнення науки і техніки для забезпечення інформаційної безпеки ПЗ; *використовувати* операційні системи, мережеві технології, засоби розробки інтерфейсу при конструюванні та захисті ПЗ.

Зміст навчальної дисципліни: Введення в безпеку програм та даних. Засоби захисту програм та даних. Криптографічний захист програм та даних. Перевірка цілісності програм і даних. Моделі розповсюдження програмного забезпечення. Пакувальники і їх відмінності від архіваторів. Основні поняття ОС, необхідні для захисту програмного забезпечення. Програмно-апаратні методи захисту ПЗ від несанкціонованого копіювання. Захист програм від несанкціонованого дослідження. Захист від дизасемблювання. Захист програм шляхом обфускації. Захист від несанкціонованого налагоджування. Сучасні технології дампінга і захисту від нього.

Пререквізити: архітектура та проектування ПЗ.

Постреквізити: професійна практика.

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для першого (бакалаврського) рівня вищої освіти за денною формою здобуття освіти становить 10 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 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: іспит.

Навчальні ресурси:

1. Безпека програм та даних: навчальний посібник/ В. І. Горбенко, А.О. Лісняк. Запоріжжя: ЗНУ, 2022. 72 с.
2. Основи інформаційної безпеки : навч. посібник/ В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
3. Основи криптології: навч. Посібник/ Н.О. Щур, О.А. Покотило. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
4. Теорія інформації і кодування: курс лекцій: навч. посіб./ А.Є.Коваленко. Київ : КПІ ім. Ігоря Сікорського, 2020. 248 с.
5. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua
6. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khmnu.edu.ua

Викладач: канд. техн. наук, доц. Тітова В.Ю.