ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

09 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології захисту інформації та кібербезпека
Назва дисципліни

Галузь знань – 12 Інформаційні технології
Спеціальність – 122 Комп'ютерні науки
Рівень вищої освіти – Перший (бакалаврський)
Освітньо-професійна програма – Комп'ютерні науки
Обсяг дисципліни – 4 кредити ЄКТС
Шифр дисципліни – ОПП.05
Мова навчання – Українська
Статус дисципліни: Обов'язкова (професійної підготовки)
Факультет – Інформаційних технологій
Кафедра – Комп'ютерних наук

Форма здобуття освіти	Курс	Семестр	Загальний обсяг		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
Д	2	4	4	120	50	16	34			70				+
Разом ДФН			**4**	**120**	**50**	**16**	**34**			**70**				**4**

Робоча програма складена на основі освітньо-професійної програми «Комп'ютерні науки» за спеціальністю 122 «Комп'ютерні науки»

Робоча програма складена _____ д-р. техн. наук, проф. Едуард МАНЗЮК .
Підпис автора Науковий ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора

Схвалена на засіданні кафедри Комп'ютерних наук

Протокол від 29.08.2025 № 1 . Зав. кафедри _____ Олександр БАРМАК
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

ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ініціали, ПРІЗВИЩЕ
Завідувач кафедри, д-р. техн. наук, проф.	Комп'ютерних наук		Олександр БАРМАК
Гарант освітньо-професійної програми, канд. техн. наук, доц.	Комп'ютерних наук		Олександр МАЗУРЕЦЬ

3. Пояснювальна записка

Дисципліна «Технології захисту інформації та кібербезпека» є однією із дисциплін фахової підготовки і займає провідне місце у підготовці здобувачів першого (бакалаврського) рівня вищої освіти, очної (денної) (далі – денної) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «Комп'ютерні науки» в межах спеціальності 122 «Комп'ютерні науки».

Пререквізити – основи програмної інженерії та тестування програмного забезпечення (ОПП.10), алгоритмізація та програмування (ОЗП.05), об'єктно-орієнтоване проєктування (ОПП.03), теорія алгоритмів (ОЗП.08).

Кореквізити – технології розподілених систем та паралельних обчислень (ОПП.11), проєктно-технологічна практика (ОПП.15), професійна практика (ОПП.16), кваліфікаційна робота (ОПП.17).

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

компетентностей: здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури. (ФК 14).

програмних результатів навчання: розуміти концепцію інформаційної безпеки, принципи безпечного проєктування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних. (ПРН 15).

Мета дисципліни. Формування у здобувачів вищої освіти компетентностей, необхідних для розв'язання складних спеціалізованих задач у сфері технологій захисту інформації та кібербезпеки, розвитку навичок застосування криптографічних методів та алгоритмів, опанування стандартів інформаційної безпеки, протоколів автентичності та систем управління безпекою інформаційних ресурсів.

Предмет дисципліни. Криптографічні алгоритми симетричного та асиметричного шифрування, хеш-функції та цифрові підписи, стандарти інформаційної безпеки ISO/IEC 17799 та FIPS 140, програмно-технічні міри забезпечення безпеки, протоколи автентичності та обміну ключів, моделі безпеки інформаційних систем, технології керування криптографічними ключами та системи контролю доступу.

Завдання дисципліни. Формування практичних навичок реалізації та аналізу класичних та сучасних алгоритмів шифрування, опанування технологій потокового та блокового шифрування з різними режимами роботи, розвитку здатностей до застосування хеш-функцій та цифрових підписів для забезпечення автентичності та цілісності даних, вивчення протоколів безпечної взаємодії та систем розподілу ключів з використанням довіреної третьої сторони.

Результати навчання. Після вивчення дисципліни студент повинен знати основні принципи криптографії та вміти застосовувати класичні алгоритми шифрування від шифру Цезаря до багатоалфавітного шифру Віжінера, розуміти математичні основи сучасних криптографічних систем та вміти реалізовувати алгоритми симетричного шифрування DES, AES та Blowfish з різними режимами роботи ECB, CBC, OFB та CTR. Студент повинен опанувати технології потокового шифрування з використанням лінійних регістрів зсуву та алгоритму RC4, розуміти принципи роботи асиметричних алгоритмів RSA та Діффі-Хеллмана, вміти застосовувати хеш-функції MD5, SHA-1, SHA-2 та SHA-3 для забезпечення цілісності даних. Необхідно вміти створювати та перевіряти цифрові підписи з використанням алгоритмів DSA та криптографії еліптичних кривих, розробляти протоколи автентичності з симетричним та асиметричним шифруванням, конфігурувати системи розподілу ключів та протоколи безпечної мережевої взаємодії. Студент повинен розуміти вимоги стандартів ISO/IEC 17799 та FIPS 140, вміти проєктувати архітектуру безпеки з урахуванням ідентифікації, автентичності, контролю доступу, протоколювання та аудиту, а також застосовувати чотирьохфазну модель процесу керування інформаційною безпекою для забезпечення комплексного захисту інформаційних систем.

4. Структура залікових кредитів дисципліни

Назва розділу (теми)	Кількість годин, відведених на:		
	Лекції	**Лаб. роботи**	**СРС**
Тема 1**.** Вступ до інформаційної безпеки. Основні програмно-технічні міри забезпечення безпеки. Стандарт FIPS 140 «Вимоги до криптографічних модулів». Стандарт ISO/IEC 17799.	4	8	11
Тема 2. Класичні алгоритми шифрування. Потокові криптосистеми.	4	8	11
Тема 3. Алгоритми симетричного шифрування.	3	6	11
Тема 4. Криптографія з відкритим ключем.	2	4	11
Тема 5**.** Хеш-функції і автентичність повідомлення. Цифровий підпис. Криптографія з використанням еліптичних кривих.	2	4	11
Тема 6. Алгоритми обміну ключів і протоколи автентичності. Протоколи безпечної мережевої взаємодії.	3	6	11
Разом:	18	36	66

5. Програма навчальної дисципліни

5.1 Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
1	Вступ до інформаційної безпеки. Основні програмно-технічні міри забезпечення безпеки. Основні поняття криптографії. Політика безпеки. Моделі мережевої безпеки. Моделі безпеки інформаційної системи. Основні поняття програмно-технічного рівня безпеки. Архітектурна безпеки. Ідентифікація та автентичність. Парольна автентичність. Керування доступом. Протоколювання і аудит. Екранування. Тунелювання. Керування. Стандарт FIPS 140 «Вимоги до криптографічних модулів». Літ.: [1] с. 9–33; [3] с. 1–35;[4] с. 14–48	2
2	Стандарт ISO/IEC 17799. Специфікація, порти та інтерфейси, ролі, сервіси і автентичність. Модель у вигляді кінцевого автомата, фізична безпека. Експлуатаційний систем, керування криптографічними ключами. Самотестування, довіра проєктуванню, стримування атак. Керування інформаційною безпекою. Практичні правила Регулятори безпеки і реалізовані ними цілі. Регулятори загального характеру. Регулятори технічного характеру. Розробка і супровід, керування безперебійною роботою, контроль відповідності. Чотирьохфазна модель процесу керування інформаційною безпекою. Літ.: [1] с. 33–58; [5] с. 37–57	2
3	Класичні алгоритми шифрування. Потокові криптосистеми. Шифр Цезаря. Частотний криптоаналіз. Шифр де ла Порта. Шифрування методом Енея. Шифр Плейфейра. Шифр Холма. Багатоалфавітній шифр Віжінера. Криптоаналіз - метод Казіскі. Шифр Вернама. Одноразовий блокнот. Літ.: [1] с. 58–79; [2] с. 251–319	2
4	Потокові шифри. Потокове шифрування Лінійний регістр зсуву із зворотнім зв'язком (LFSR). LFSR статистичні властивості. Комбінаторний генератор. Алгоритм RC4. Режими шифрування блокових шифрів. ECB: Electronic Codebook. CBC: Cipher Block Chaining (зчеплення шифрованих блоків). OFB: Output Feedback Mode (зворотний зв'язок за виходом). CTR: Counter Mode (зустрічний режим). Літ.: [1] с. 138–160; [2] с. 340–355, 397–403	2
5	Алгоритми симетричного шифрування. Основні вимоги, що ставляться до алгоритмів симетричного шифрування. Визначення стійкості алгоритму. Мережа Фейштеля. Основні поняття криптоанализа (лінійний і диференціальний криптоаналіз). Опис алгоритмів DES і потрійного DES. Алгоритм Blowfish. Режими виконання алгоритмів симетричного шифрування. Створення випадкових чисел. Криптографічно створені випадкові числа. Алгоритм Rijndael. Математичні конструкції алгоритму. Обґрунтування розробки. Специфікація алгоритму. Літ.: [1] с. 79–107; [2] с. 331–340, 375–389	2
6	Криптографія з відкритим ключем. Основні вимоги до алгоритмів асиметричного шифрування. Алгоритм RSA (Rivest-Shamir-Adleman). Алгоритм обміну ключа Діффі-Хеллмана. Літ.: [1] с. 160–171; [2] с. 403–457	2
7	Хеш-функції і автентичність повідомлення. Вимого до хеш-функцій. "Парадокс дня народження". Хеш-функція MD5. Хеш-функція SHA-1, SHA-2. Коди автентичності – MAC. Нова структура SHA-3. Літ.: [1] с. 171–208; [2] с. 519–551	2
8	Цифровий підпис. Криптографія з використанням еліптичних кривих. Вимоги до цифрового підпису. Прямий та арбітражний цифровий підпис. Стандарт цифрового підпису DSS (Digital Signature Algorithm). Літ.: [1] с. 208–263; [2] с. 483–519	2

9	Алгоритми обміну ключів і протоколи автентичності. Алгоритми розподілу ключів з використанням третьої сторони. Протоколи автентичності. Використання симетричного шифрування. Використання шифрування з відкритим ключем. Одностороння автентичність. Протоколи безпечної мережевої взаємодії. Функції AS та TGS. Структура (ticket). Літ.: [1] с. 229– 263, с. 306– 369; [2] с. 454-459	2
	Разом:	18

5.2 Зміст лабораторних занять

№ п/п	Тема лабораторного заняття	Годин
1	Класичні алгоритми шифрування. Літ.: [6] с. 7–29	4
2	Потокові криптосистеми. Літ.: [6] с. 29–44	4
3	Блочні системи шифрування. Стандарт AES (Advanced Encryption Standard) – алгоритм Rijndael. Літ.: [1] с. 99–107; [6] с. 44–59	8
4	Асиметричні системи шифрування. Алгоритм RSA. Літ.: [1] с. 160–168; [6] с. 59–68	4
5	Хеш-функції. Літ.: [1] с. 192–208; [6] с. 68–83	4
6	Електронний цифровий підпис. Літ.: [1] с. 229–231; [6] с. 83–89	8
7	Криптосистеми, які ґрунтуються на еліптичних кривих Літ.: [6] с. 89–100	4
	Разом:	36

5.3 Зміст самостійної (у т.ч. індивідуальної) роботи здобувача вищої освіти

Самостійна робота студентів усіх форм здобуття освіти полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до виконання і захисту лабораторних робіт. Крім цього до послуг студентів сторінка навчальної дисципліни у Модульному середовищі для навчання, де розміщені Робоча програма дисципліни та необхідні документи з її навчально-методичного забезпечення.

Номер тижня	Вид самостійної роботи	Кількість годин
1–2	Опрацювання теоретичного матеріалу, підготовка до проведення лабораторної роботи та її захисту, а також виконання індивідуального завдання.	8
3-4	Опрацювання теоретичного матеріалу, підготовка до проведення лабораторної роботи та її захисту, а також виконання індивідуального завдання.	8
5-6	Опрацювання теоретичного матеріалу, підготовка до проведення лабораторної роботи та її захисту, а також виконання індивідуального завдання.	8
7-8	Опрацювання теоретичного матеріалу, підготовка до проведення лабораторної роботи та її захисту, а також виконання індивідуального завдання.	8
9-10	Опрацювання теоретичного матеріалу, підготовка до проведення лабораторної роботи та її захисту, а також виконання індивідуального завдання.	8
11-12	Опрацювання теоретичного матеріалу, підготовка до проведення лабораторної роботи та її захисту, а також виконання індивідуального завдання.	8
13-14	Опрацювання теоретичного матеріалу, підготовка до проведення лабораторної роботи та її захисту, а також виконання індивідуального завдання.	8
15-16	Опрацювання теоретичного матеріалу, підготовка до підсумкового контрольного заходу. Захист індивідуального завдання.	10
	Разом:	66

На самостійне опрацювання студентів виносяться визначені у методичних рекомендаціях до лабораторних занять та самостійної роботи індивідуальні завдання (ІЗ) (з відповідних тем. Керівництво самостійною роботою та конт-

роль за виконанням індивідуального завдання здійснюється викладачем згідно з розкладом консультацій у позаурочний час.

Вимоги до виконання індивідуального завдання викладені в Модульному середовищі для навчання на сторінці навчальної дисципліни.

6. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій та методів навчання, зокрема: лекції (з використанням методів візуалізації, проблемного навчання, мотиваційних прийомів, інформаційно-комунікаційних технологій); лабораторні заняття: з використанням методів комп'ютерного моделювання, аналіз проблемних ситуацій, пояснення, дискусія тощо, самостійна робота: робота над засвоєнням теоретичного матеріалу, виконання індивідуальних та домашніх завдань, підготовка до поточного та підсумкового контролю тощо), , з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

7. Методи контролю

Поточний контроль здійснюється під час аудиторних 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;
- оцінювання індивідуальних завдань.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контролю, 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 обсяг роботи, передбачений Робочою програмою. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу) 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 лабораторного заняття (вивчення теоретичного матеріалу з теми роботи, попередню підготовку протоколу роботи, (наведені у Методичних рекомендаціях до лабораторних занять)), активно працювати на занятті, якісно підготувати звіт (протокол роботи відповідно до теми), захистити результати виконаної роботи, брати участь у дискусіях щодо прийнятих конструктивних рішень при виконанні здобувачами лабораторних робіт тощо.

Здобувачі вищої освіти мають дотримуватися встановлених термінів виконання всіх видів навчальної роботи відповідно до робочої програми навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо студент захистив її на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами опитування під час захисту лабораторних робіт та контрольної роботи.

Здобувач вищої освіти, виконуючи самостійну роботу або індивідуальну роботу з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення порушення політики академічної доброчесності 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, 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).

Окремі теми курсу можуть бути зараховані у випадку отримання студентом **результатів навчання у неформальній освіті**, що підтверджені відповідним документом (сертифікат, свідоцтво, освітня програма тощо) та відповідно до Положення про порядок визнання та перезарахування результатів навчання здобувачів вищої освіти у ХНУ

(https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-poryadok-vyznannya-ta-perezarahuvannya-rezultativ-navchannya.pdf). Перелік лабораторних робіт, що можуть бути перезараховані та приклади відповідних курсів на освітніх ресурсах:
Лабораторні роботи 2, 3, 6: Stanford University Cryptography I https://www.coursera.org/learn/crypto#modules.
Лабораторні роботи 3-7: Cryptography https://www.coursera.org/learn/cryptography**.**

9. Оцінювання результатів навчання студентів у семестрі

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». 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.

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 студентів денної форми здобуття освіти у семестрі

Лабораторна робота							**Самостійна робота**	**Семестровий контроль**	**Разом**
							ІЗ	**Іспит**	Сума балів
1	2	3	4	5	6	7	1		
3-5	3-5	3-5	3-5	3-5	3-5	3-5	15-25	24-40	**60-100***
21-35							**15-25**	**24-40**	

Примітки: *За набрану з будь-якого виду навчальної роботи з 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; знання теоретичного матеріалу; здатність аргументувати прийняті рішення; повнота та якість отриманих результатів; дотримання вимог до оформлення та структурування роботи; уміння виправляти виявлені помилки у ході захисту.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці "Критеріїв оцінювання навчальних досягнень здобувача вищої освіти" (мінімальний позитивний бал – 3 бали, максимальний – 5 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 виконання індивідуального завдання

Виконане та оформлене відповідно до вимог, визначених Методичними рекомендаціями, індивідуальне завдання (ІЗ) комплексно оцінюється викладачем з урахуванням таких критеріїв: самостійність виконання; правильність розв'язання поставлених задач; обґрунтованість вибору методів розв'язання; повнота пояснень та аргументованість відповідей; якість оформлення та дотримання вимог до структури і змісту роботи.

Результат виконання здобувачем вищої освіти кожного ІЗ оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти з урахуванням рівня досягнення запланованих програмних результатів навчання та сформованих компетентностей. За підсумками захисту присвоюється відповідна сума балів (мінімальний позитивний бал – 15 балів, максимальний – 25 балів).

У разі, якщо здобувач вищої освіти виявив рівень знань і виконання ІЗ, що нижчий ніж 60 відсотків від максимальної кількості балів, встановленої Робочою програмою для цієї структурної одиниці, завдання не зараховується. У такому випадку студент має повторно опрацювати зміст завдання, усунути помилки та здати на перевірку доопрацьоване ІЗ у терміни, погоджені з викладачем.

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 як теоретичної, так і практичної підготовки здобувача з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами. Відповідно до цього в екзаменаційному білеті пропонується поєднання питань як теоретичного (в т.ч. у тестовій формі), так і практичного характеру.

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів денної форми навчання (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	3	4	5
Теоретичне питання № 2	3	4	5
Практичне завдання	18	24	30
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)**.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання у балах з усіх видів навчальної роботи до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС наведені нижче у таблиці «Співвідношення».

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав студент з дисципліни за результатами поточного 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 студентом сумі балів відповідно до таблиці Співвідношення.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Рейтингова шкала балів**	**Інституційна оцінка** (рівень 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 ***Задовільно*/*Satisfactory*** – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни
C	73-82		
D	66-72		
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

10. Питання для самоконтролю результатів навчання

1. Основні поняття криптографії.
2. Політика безпеки.
3. Моделі мережевої безпеки.
4. Моделі безпеки інформаційної системи.
5. Основні програмно-технічні міри забезпечення безпеки.
6. Основні поняття програмно-технічного рівня безпеки.
7. Архітектурна безпеки.
8. Ідентифікація та автентичність.
9. Парольна автентичність.
10. Керування доступом.
11. Протоколювання і аудит.
12. Екранування.
13. Тунелювання. Керування.
14. Стандарт FIPS 140 «Вимоги до криптографічних модулів».
15. Специфікація, порти та інтерфейси, ролі, сервіси і автентичність.
16. Модель у вигляді кінцевого автомата, фізична безпека.
17. Експлуатаційний систем, керування криптографічними ключами.
18. Самотестування, довіря проектуванню, стримування атак.
19. Стандарт ISO/IEC 17799.
20. Керування інформаційною безпекою.
21. Практичні правила – регулятори безпеки і реалізовані ними цілі.
22. Регулятори загального характеру.
23. Регулятори технічного характеру.
24. Розробка і супровід, керування безперебійною роботою, контроль відповідності.
25. Чотирьохфазна модель процесу керування інформаційною безпекою.
26. Класичні алгоритми шифрування.
27. Шифр Цезаря.
28. Частотний криптоаналіз.
29. Шифр де ла Порта.
30. Шифрування методом Енея.
31. Шифр Плейфейра.
32. Шифр Холма.
33. Багатоалфавітній шифр Віжінера.
34. Криптоаналіз - метод Казискі.
35. Шифр Вернама.
36. Одноразовий блокнот
37. Алгоритми симетричного шифрування.
38. Основні вимоги, що ставляться до алгоритмів симетричного шифрування.
39. Визначення стійкості алгоритму.
40. Мережа Фейштеля.

41. Основні поняття криптоанализа (лінійний і диференціальний криптоаналіз).
42. Опис алгоритмів DES і потрійного DES.
43. Алгоритм Blowfish.
44. Режими виконання алгоритмів симетричного шифрування.
45. Створення випадкових чисел.
46. Криптографічно створені випадкові числа.
47. Генератор псевдовипадкових чисел ANSI X9.17
48. Потокові криптосистеми.
49. Потокові шифри. Потокове шифрування
50. Лінійний регістр зсуву із зворотнім зв'язком (LFSR).
51. LFSR статистичні властивості.
52. Комбінаторний генератор.
53. Алгоритм RC4.
54. ECB: Electronic Codebook.
55. CBC: Cipher Block Chaining (зчеплення шифрованих блоків).
56. OFB: Output Feedback Mode (зворотний зв'язок за виходом).
57. CTR: Counter Mode (зустрічний режим).
58. Математичні конструкції алгоритму Rijndael.
59. Обґрунтування розробки Rijndael.
60. Специфікація алгоритму Rijndael.
61. Основні вимоги до алгоритмів асиметричного шифрування.
62. Алгоритм RSA (Rivest-Shamir-Adleman).
63. Алгоритм обміну ключа Діффі-Хеллмана.
64. Вимого до хеш-функцій.
65. "Парадокс дня народження".
66. Хеш-функція MD5.
67. Алгоритм MD4.
68. Хеш-функція SHA-1, SHA-2, SHA-3
69. Коди автентичності – MAC.
70. Вимоги до цифрового підпису.
71. Прямий та арбітражний цифровий підпис.
72. Стандарт цифрового підпису DSS (Digital Signature Algorithm).
73. Математичні основи криптосистем з використанням еліптичних кривих.
74. Аналог алгоритму Діффі-Хеллмана обміну ключами.
75. Шифрування/дешифрування з використанням еліптичних кривих.
76. Алгоритми розподілу ключів з використанням третьої сторони.
77. Протоколи автентичності.
78. Використання симетричного шифрування.
79. Використання шифрування з відкритим ключем.
80. Одностороння автентичність.

11. Навчально-методичне забезпечення

Освітній процес з дисципліни «Технології захисту інформації та кібербезпека» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою. Зокрема, викладачами кафедри підготовлені і видані такі роботи:

1. Технології захисту інформації та кібербезпека: методичні рекомендації до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 122 «Комп'ютерні науки» / Е. А. Манзюк, О. А. Пасічник, В. Ц. Міхалевський, Т. К. Скрипник, С. С. Петровський. Хмельницький : ХНУ, 2024. 116 с.
2. Курс «Технології захисту інформації та кібербезпека». https://msn.khmnu.edu.ua/course/view.php?id=424

12. Матеріально-технічне та програмне забезпечення дисципліни (за потреби)

Необхідні інструменти, обладнання, програмне забезпечення: комп'ютер (надається для використання в лабораторіях кафедри комп'ютерних наук), Visual Studio (ліцензія ХНУ), текстовий редактор (пропонується використання безкоштовних онлайн-сервісів); виконувати лабораторні роботи та індивідуальні завдання студенти можуть на мові програмування за власним вибором.

13. Рекомендована література:

Основна

1. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2025. – 678 с.
2. Кібербезпека: основи кодування та криптографії: навчальний посібник / С.П. Євсеєв, О.В. Мілов, С.Е. Оста-

пов, О.В. Сєвєрінов. – Харків: Вид. “Новий Світ-2000”, 2024. – 658 с.

3. Goyal S. B., Kumar V., Islam S. M. N., Ghai D. Quantum Computing, Cyber Security and Cryptography: Issues, Technologies, Algorithms, Programming and Strategies: Springer Nature Singapore, 2025. 504p.

4. Stapleton, Jeff, and W. Clay Epstein. Security without Obscurity: A Guide to PKI Operations. CRC Press, 2024. 312 p.

5. Sharp, Robin. Introduction to Cybersecurity: A Multidisciplinary Challenge. Springer Nature, 2023. 452 p.

6. Технології захисту інформації та кібербезпека: методичні рекомендації до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 122 «Комп’ютерні науки» / Е. А. Манзюк, О. А. Пасічник, В. Ц. Міхалевський, Т. К. Скрипник, С. С. Петровський. Хмельницький : ХНУ, 2024. 116 с.

Додаткова

7. Mammeri Z. Cryptography. Algorithms, Protocols, and Standards for Computer Security / Z. Mammeri. – Wiley, 2024. – 616 p.

8. Bertaccini M. Cryptography Algorithms / M. Bertaccini. – Packt Publishing, 2022. – 358 p.

9. Additional Diffie-Hellman Groups for Use with IETF Standards. RFC 5114.2018.

10. ANSI X9.102-2020 Symmetric Key Cryptography For The Financial Services Industry – Wrapping Of Keys And Associated Data, 2020.

11. ANSI X9.142-2020, Financial Services – Public Key Cryptography For The Financial Services Industry – The Elliptic Curve Digital Signature Algorithm – ECDSA, 2020.

12. FIPS PUB 180-4: Secure Hash Standard. Federal Information Processing Standards Publication 180-4, 2015.

13. FIPS PUB 186-5: Digital Signature Standard. Federal Information Processing Standards Publication 186-5, 2023.

14. FIPS 197-upd1, Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, 2023.

15. RFC 1321: The MD5 Message-Digest Algorithm, 2020.

16. Daniel R. L. Brown , Sean Turner, Elliptic Curve Private Key Structure. RFC 5915, 2020.

17. CompactECC – Elliptic Curve Cryptography, Reference Manual, 2010, Revision 1.4.

18. SEC 1. Elliptic Curve Cryptography. Standards for Efficient Cryptography Group, February, 2009, Working Draft. Version 2.0.

19. SEC 2. Recommended Elliptic Curve Domain Parameters. Standards for Efficient Cryptography Group, September, 2010. Version 2.0.

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL: https://msn.khmnu.edu.ua/course/view.php?id=424
2. Електронна бібліотека ХНУ. URL: http://library.khmnu.edu.ua
3. Інституційний репозитарій ХНУ. URL: https://elar.khmnu.edu.ua/home

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКА

Тип дисципліни	Обов'язкова
Освітній рівень	Перший (бакалаврський)
Мова навчання	Українська
Семестр	4
Кількість встановлених кредитів ЄКТС	4
Форми навчання, для яких викладається дисципліна	Очна (денна)

Результати навчання. Після вивчення дисципліни студент повинен знати основні принципи криптографії та вміти застосовувати класичні алгоритми шифрування від шифру Цезаря до багатоалфавітного шифру Віжінера, розуміти математичні основи сучасних криптографічних систем та вміти реалізовувати алгоритми симетричного шифрування DES, AES та Blowfish з різними режимами роботи ECB, CBC, OFB та CTR. Студент повинен опанувати технології потокового шифрування з використанням лінійних регістрів зсуву та алгоритму RC4, розуміти принципи роботи асиметричних алгоритмів RSA та Діффі-Хеллмана, вміти застосовувати хеш-функції MD5, SHA-1, SHA-2 та SHA-3 для забезпечення цілісності даних. Необхідно вміти створювати та перевіряти цифрові підписи з використанням алгоритмів DSA та криптографії еліптичних кривих, розробляти протоколи автентичності з симетричним та асиметричним шифруванням, конфігурувати системи розподілу ключів та протоколи безпечної мережевої взаємодії. Студент повинен розуміти вимоги стандартів ISO/IEC 17799 та FIPS 140, вміти проєктувати архітектуру безпеки з урахуванням ідентифікації, автентичності, контролю доступу, протоколювання та аудиту, а також застосовувати чотирьохфазну модель процесу керування інформаційною безпекою для забезпечення комплексного захисту інформаційних систем.

Зміст навчальної дисципліни. Основні поняття криптографії. Політика безпеки. Моделі мережевої безпеки. Моделі безпеки інформаційної системи. Основні поняття програмно-технічного рівня безпеки. Архітектура безпеки. Ідентифікація та автентичність. Стандарт FIPS 140. Стандарт BS 7799 (ISO/IEC 17799). Класичні алгоритми шифрування. Алгоритми симетричного шифрування. Потокові криптосистеми. Хеш-функції і автентичність повідомлення. Цифровий підпис. Алгоритми обміну ключів і протоколи автентичності. Протоколи безпечної мережевої взаємодії.

Пререквізити – основи програмної інженерії та тестування програмного забезпечення (ОПП.10), алгоритмізація та програмування (ОЗП.05), об'єктно-орієнтоване проєктування (ОПП.03), теорія алгоритмів (ОЗП.08).

Кореквізити – технології розподілених систем та паралельних обчислень (ОПП.11), проєктно-технологічна практика (ОПП.15), професійна практика (ОПП.16), кваліфікаційна робота (ОПП.17).

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 методів візуалізації, проблемного навчання, мотиваційних прийомів, інформаційно-комунікаційних технологій); лабораторні заняття: з використанням методів комп'ютерного моделювання, аналіз проблемних ситуацій, пояснення, дискусія тощо, самостійна робота: робота над засвоєнням теоретичного матеріалу, виконання індивідуальних та домашніх завдань, підготовка до поточного та підсумкового контролю тощо) з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

Форми оцінювання результатів навчання: захист лабораторних робіт.

Вид семестрового контролю іспит.

Навчальні ресурси:

1. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих на-вчальних закладів. / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2025. – 678 с.

2. Кібербезпека: основи кодування та криптографії: навчальний посібник / С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2024. – 658 с.

3. Goyal S. B., Kumar V., Islam S. M. N., Ghai D. Quantum Computing, Cyber Security and Cryptography: Issues, Techn-?logies, Algorithms, Programming and Strategies: Springer Nature Singapore, 2025. 504p.

4. Stapleton, Jeff, and W. Clay Epstein. Security without Obscurity: A Guide to PKI Operations. CRC Press, 2024. 312 p.

5. Sharp, Robin. Introduction to Cybersecurity: A Multidisciplinary Challenge. Springer Nature, 2023. 452 p.

6. Технології захисту інформації та кібербезпека: методичні рекомендації до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 122 «Комп'ютерні науки» / Е. А. Манзюк, О. А. Пасічник, В. Ц. Міхалевський, Т. К. Скрипник, С. С. Петровський. Хмельницький : ХНУ, 2024. 116 с.

7. Модульне середовище для навчання. URL: https://msn.khmnu.edu.ua/course/view.php?id=424
8. Електронна бібліотека університету. URL: http://library.khmnu.edu.ua

Викладач: д-р. техн. н., проф., Едуард МАНЗЮК