ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

29 серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Програмування криптографічних алгоритмів

Призначення робочої програми – Для освітніх програм різних спеціальностей
Рівень вищої освіти – Перший (бакалаврський)
Обсяг дисципліни – 8 кредитів ЄКТС
Мова навчання – Українська
Статус дисципліни – Вибіркова
Факультет – Інформаційних технологій
Кафедра – Кібербезпеки

Форма здобуття освіти	Загальний обсяг		Кількість годин						Форма семестрового контролю
			Аудиторні заняття					Самостійна робота, у т.ч. ІРС	Залік
	Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття		
Д	8	240	82	32	32	18	-	158	+
Разом ДФН	**8**	**240**	**82**	**32**	**32**	**18**	**-**	**158**	**1**

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

Робоча програма складена _____ канд. техн. наук, доцент Володимир ДЖУЛІЙ
Підпис Науковий ступінь, учене звання Ім'я, ПРІЗВИЩЕ

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 29.08.2025 № 1. Зав. кафедри _____ Юрій КЛЬОЦ

Хмельницький 2025

3. Пояснювальна записка

Дисципліна "Програмування криптографічних алгоритмів" відноситься до циклу вибіркових дисциплін та сприяє поглибленню фахових умінь зі створення ефективних криптографічних алгоритмів, засвоєнню сучасних технологій і підходів у сфері кібербезпеки та захисту інформації, а також набуттю практичних навичок програмування, тестування та оптимізації програмного коду. Опанування дисципліни формує готовність до подальшої професійної спеціалізації, розвиває мовну підготовку через роботу з технічною документацією, інтерфейсами та стандартами. У процесі навчання здобувачі набувають важливих соціальних навичок (soft skills): уміння комунікувати, працювати в команді, проявляти ініціативу, брати відповідальність і приймати рішення в умовах реальних проєктних завдань. є етапом підготовки до самостійної практичної діяльності з розробки і експлуатації безпечних програмних додатків, є етапом підготовки до самостійної практичної діяльності з розробки і екплуатації безпечних програмних додатків.

Мета дисципліни. Формування системи знань та розуміння предметної області щодо процесів в галузі інформаційних технологій, що охоплює сучасні методи та підходи до розробки алгоритмів захисту інформації та їх практичному використанню при проектуванні систем захисту інформації, методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності; практичному використанню програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

Предмет дисципліни. Сучасні інформаційні технологій у галузі інформаційної безпеки та криптографічні методи захисту інформації. Алгоритми реалізації основних методів захисту інформації, сучасних криптографічних протоколів. Методи та моделі інформаційної безпеки та/або кібербезпеки. Сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій у природничій і загально-професійній галузях інформаційної та/або кібербезпеки.

Завдання дисципліни. Показати студентам сучасний стан методів, технологій розробки і проектування криптографічних алгоритмів захисту інформації в середовищі електронно-обчислювальних систем і мереж. Навчити застосовувати методи та моделі інформаційної безпеки та/або кібербезпеки, алгоритми реалізації основних методів захисту інформації та сучасних криптографічних протоколів. Забезпечити набуття компетентностей та досягнення результатів навчання.

Результати навчання. Після вивчення дисципліни студент повинен:: *застосовувати* знання алгоритмів захисту інформації і технологій їх програмної реалізації у практичних ситуаціях, адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; використовувати програмні та програмно-апаратні комплекси засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах, *обирати* відповідну технологію програмування і *виконувати* аналіз специфікації задач, *вирішувати* завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень, *забезпечувати* функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності, *вирішувати* задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних методів та засобів криптографічного захисту інформації, *виконувати* впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; *використовувати* інформаційно-комунікаційні технології, сучасні методи і моделі інформаційної безпеки та/або кібербезпеки, *застосовувати* теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

4. Структура залікових кредитів дисципліни

Назва розділу (теми)	Кількість годин, відведених на:			
	лекції	лабораторні	практичні	СРС
Тема 1. Основні поняття інформаційної безпеки. Класифікація методів та алгоритмів захисту інформації. Основи криптографії та криптоаналізу.	8	6	8	24
Тема 2. Ідентифікація й аутентифікація. Поняття протоколу ідентифікації. Ідентифікуюча інформація.	4	8	2	30
Тема 3. Криптографія з відкритим ключем. Алгоритми асиметричного шифрування. Хеш – функції і аутентифікація повідомлень	8	8	4	30
Тема 4. Цифрова підпис. Стандарт цифрового підпису. Протоколи аутентифікації.	8	2	2	34
Тема 5. Керування ризиками й побудова систем мережної безпеки	4	8	2	40
Разом:	**32**	**32**	**18**	**158**

5. Програма навчальної дисципліни

5.1 Зміст лекційного курсу

Номер лекції	Перелік змістових модулів, тем лекцій, їх анотації	Кількість годин
	Тема 1. Основні поняття інформаційної безпеки. Класифікація методів та алгоритмів захисту інформації. Основи криптографії та криптоаналізу.	**8**
1	**Основні поняття і визначення інформаційної безпеки**: атаки, вразливості, політика безпеки, механізми й сервіси безпеки. Модель мережної безпеки. Класифікація методів та алгоритмів захисту інформації Літ.:[1] с.11-14; [6] с.23-92; [7] с.2-14;	2
2	**Класифікація мережних атак. Модель мережної взаємодії. Псевдовипадкові числа** Сервіси безпеки. Модель безпеки інформаційної системи. Вимоги до випадкових чисел. Генератори псевдовипадкових чисел. Криптографічно створені випадкові числа. Літ.:[5] с.11-25; [6] с.23-139; [7] с.2-14;	2
3	**Аналіз основних криптографічних методів захисту інформації**. **Стиснення інформації.** Основні поняття. Класифікація криптографічних методів. Криптографічні методи захисту інформації. Стиснення інформації як один з методів її захисту. Алгоритми архівації даних. Стиснення способом кодування серій (RLE). Алгоритм Хаффмана Літ.:[5] с.133-145; [6] с.148-155;	2
4	**Алгоритми симетричного шифрування. Криптографія**. Мережа Фейштеля. Криптоаналіз. Диференціальний і лінійний криптоаналіз. Використовувані критерії при розробці алгоритмів Літ.:[5] с.133-145; [6] с.148-155;	2
	Тема 2. Ідентифікація й аутентифікація. Поняття протоколу ідентифікації. Ідентифікуюча інформація.	**4**
5	**Ідентифікація й аутентифікація. Поняття протоколу ідентифікації**. Ідентифікуюча інформація. Паролі. Основні поняття й класифікація. Проста аутентифікація. Аутентифікація на основі багаторазових паролів. Літ.:[5] с.209 - 324; [6] с.171-235;	2
6	**Аутентифікація на основі одноразових паролів**, аутентифікація на основі сертифікатів. Біометрична ідентифікація й аутентифікація користувачів. Літ.:[5] с.209 -324; [6] с.171-235;	2
	Тема 3. Криптографія з відкритим ключем. Алгоритми асиметричного шифрування. Хеш – функції і аутентифікація повідомлень	**8**
7	**Основні поняття і визначення інформаційної безпеки Криптографія з відкритим ключем.** Модель мережної взаємодії. Основні поняття. Визначення. Асиметричні алгоритми. Відкритий, закритий ключі. Літ.:[1] с.11-14, с.133-145;; [2] с.148-155; [6] с.23-92; [7] с.2-14;	2

8	**Криптографія з відкритим ключем. Алгоритм обміну ключами** Основні вимоги до алгоритмів асиметричного шифрування. Алгоритм RSA. Діфі-Хелмана. Цифровий (електронний) підпис на основі криптосистеми RSA. Літ.:[1] с.133-145; [2] с.148-155;	2
9	**Хеш-функції й аутентифікація повідомлень**. Хеш-функції. Вимоги до хеш-функцій. Прості хеш-функції. Хеш-функції, основані на створенні ланцюжка зашифрованих блоків. Хеш-функція MD5. Літ.:[1] с.151-185; [2] с.155-167;	2
10	**Хеш-функції.**. Хеш-функції SHA-2, SHA-384, SHA-512, SHA-1024 Літ.:[1] с.167-185; [2] с.155-167;	2
	Тема 4. Цифрова підпис. Стандарт цифрового підпису. Протоколи аутентифікації.	**8**
11	**Цифровий підпис. Вимоги до цифрового підпису**. **Стандарт цифрового підпису DSS**. Пряма й арбітражна цифрові підписи. Стандарт цифрового підпису ГОСТ 3410. Літ.: [1] с.209-424; [2] с.162-171;	2
12	**Алгоритми обміну ключів і протоколи аутентифікації**. Протоколи аутентифікації. Протокол Нідхема й Шредера. Протокол Деннінга. Літ.:[1] с.209-424; [2] с.162-171;	2
13	**Алгоритми обміну ключів і протоколи аутентифікації**. Протоколи аутентифікації. Алгоритми розподілу ключів з використанням третьої довіреної сторони. Літ.:[1] с.209-424; [2] с.162-171;	2
14	**Технології аутентифікації.** Протокол аутентифікації з використанням квитка. Аутентификация, авторизація й адміністрування дій користувачів. Використання шифрування з відкритим ключем. Літ.:[1] с.443-543;	2
	Тема 5. Керування ризиками й побудова систем мережної безпеки	**4**
15	**Керування ризиками й побудова систем мережної безпеки**. Методологія побудови системи інформаційної безпеки Аналіз і керування ризиками. Основні поняття й визначення. Технологія аналізу й керування ризиками. Літ.:[2] с.531-548; [8] с.269-273; [9] с.605-706;	2
16	**Керування ризиками й побудова систем мережної безпеки**. Засоби автоматизації оцінки інформаційних ризиків. підприємства. Завдання інформаційної безпеки. Модель побудови системи інформаційної безпеки. Етапи побудови системи інформаційної безпеки. Літ.:[1] с.531-548; [8] с.269-273; [9] с.605-706;	2
	Разом за семестр:	**32**

5.2 Зміст практичних занять

№ п/п	Тема практичних занять	Кільк. годин
Наскрізна практична робота: захист програмного забезпечення від нелегального копіювання. Програмна реалізація TRIAL-версії програми та програмно –апаратної прив'язки до ПК. Для взаємодії в мережі використовувати технології на основі сокетних протоколів https://msn.khnu.km.ua/course/view.php?id=5632		
1	Створити прикладне програмне забезпечення. Дана частина роботи може мати довільну реалізацію. Необхідно створити деяку програму, будь то калькулятор, шифратор, редактор файлів, провідник, браузер, що б викликало практичний інтерес у користувача. Також на етапі планування слід передбачити який функціонал буде доступний у демо-версії, який – у пробній, а який – у повній версії. Для прикладу, створимо програму-шифратор з генератором паролів. У демо-версії задамо обмеження на довжину генерованого пароля, а також на деякий інший функціонал.	2
2	Створити бібліотеку класів (DLL). Генератор паролів. Створити власний генератор випадкових простих чисел, для генерації простих чисел а також ключів шифрування. Розмістити у власну бібліотеку класів - MyLibraryFunctions**.**	2
3	На прикладі DES реалізувати власний алгоритм шифрування. Реалізувати власну утворюючу функцією ***f***. Реалізувати алгоритм шифрування/дешифрування на основі символьного потоку та на основі байтового потоку. Провести порівняння. Розширена мережа Фейстеля з трьома підблоками. Алгоритм розширення ключа.	2
4	Алгоритм RSA. Хеш-функція. Програмна реалізація. Клас Info. Шифрування файлів. Забезпечення цілісності файла. Об'єднання створених елементів керування на головній формі. Розмежування функціоналу повної та безкоштовної версії ПЗ. Вітальна форма. Форма «покупки» повної версії ПЗ.	2
5	Робота з реєстром. Клас Registry. Технологія WMI. Отримання повної інформацію про наявність портів, частоті процесора, оперативної пам'яті, системного каталогу, каталогу Windows. Технологія WQL.	2
6	Робота з мережами в C# і .NET. Адреса в .NET. Сокети. Клас Socket. Клієнт-серверний додаток на сокетах TCP.	2
7	Програмна реалізація сервера. Налагодження взаємодії клієнтської програми та сервера Авторизація та створення безпечного каналу зв'язку	2
8	Реєстрація нового клієнта. Клас Hesh на сервері. Активація токена. Активація пробного періоду. Деактивація пробного періоду. Активація повної версії	4
	Разом за семестр:	**18**

5.3 Зміст лабораторних занять

№ п/п	Тема лабораторного заняття	Кільк. годин
1	**Методи генерації псевдовипадкових чисел**. Криптографія. Класичні системи шифрування. Літ.:[5] с.209 -324; [6] с.171-235;	4
2	**Потокові алгоритми шифрування**. Реалізація потокових алгоритмів шифрування. Мережа Фейстеля Літ.:[5] с.209 -324; [6] с.171-235;	4
3	**Блочні шифри**. Реалізація режимів роботи блочних шифрів Реалізація симетричних блокових алгоритмів у CryproAPI. Літ.:[5] с.209 -324; [6] с.171-235;	4
4	**Хеш функції**. Програмна реалізація Хеш-функцій. Розробити схематичне подання хеш-функції. Розробити програмне забезпечення. Літ.:[1] с.269-498;	4
5	**Електронний цифровий підпис RSA**. Програмна реалізація електронного цифрового підпису RSA. Літ.:[1] с.269-498;	4
6	**Криптографія на еліптичних кривих**. Криптосистеми, засновані на еліптичних кривих. Ознайомитися з принципом функціонування криптосистем, заснованих на еліптичних кривих. Літ.:[1] с.443-543; [2] с.171-205;	4
7	**Криптографія на еліптичних кривих(продовження)** Реалізувати обмін ключами з використанням еліптичних кривих, а також процедуру шифрування/дешифрування, що використовує даний ключ. Літ.:[1] с.443-543; [2] с.171-205;	4
8	**Криптографія на еліптичних кривих (продовження)**Реалізувати електронно-цифрову підпис з використанням еліптичних кривих Літ.:[1] с.443-543; [2] с.171-205;	4
	Разом за семестр:	**32**

5.4 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 практичних занять, підготовці до виконання і захисту лабораторних робіт, тестування. До послуг студентів сторінка кафедри у Модульному середовищі для навчання, де розміщені Робоча програма дисципліни та необхідні матеріали з її навчально-методичного забезпечення та контролю результатів навчання.

Номер тижня	Вид самостійної роботи	Кількість годин
1-2	Опрацювання лекційного матеріалу. Підготовка до ЛР1 та ПЗ1. Підготовка до захисту ЛР1.	10
3-4	Опрацювання лекційного матеріалу. Підготовка до ЛР2 та ПЗ2. Підготовка до захисту ЛР2.	14
5-6	Опрацювання лекційного матеріалу. Підготовка до ЛР3 та ПЗ3. Підготовка до захисту ЛР3	22
7-8	Опрацювання лекційного матеріалу. Підготовка до ЛР4 та ПЗ4. Підготовка до захисту ЛР4.	22
9-10	Опрацювання лекційного матеріалу. Підготовка до ЛР5 та ПЗ5. Підготовка до захисту ЛР5	20
11-12	Опрацювання лекційного матеріалу. Підготовка до ЛР6 та ПЗ6. Підготовка до захисту ЛР6.	20
13-14	Опрацювання лекційного матеріалу. Підготовка до ЛР7 та ПЗ7. Підготовка до захисту ЛР7.	20
15-16	Опрацювання лекційного матеріалу. Підготовка до ЛР8 та ПЗ8. Підготовка до захисту ЛР8	20
17	Опрацювання лекційного матеріалу. Підготовка до ПЗ8 та тестування.	10
	Разом:	**158**

***Примітки*:** ЛР – лабораторна робота, ПЗ– практичне заняття.

На самостійне опрацювання студентів виносяться визначені у методичних рекомендаціях до практичних та лабораторних занять та самостійної роботи питання з кожної теми.

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 й інтерактивного навчання, мотиваційних прийомів, інформаційно-комунікаційних технологій); практичні заняття (з використанням інструктування, демонстрування, розв'язування типових і прикладних задач, аналізу кейсів, ситуаційних завдань, елементів дискусії тощо); самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання практичних робіт, поточного та підсумкового контролю, виконання індивідуальних та домашніх завдань), з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

7. Методи контролю

Поточний контроль здійснюється під час аудиторних практичних та 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 роботи на практичних заняттях (опитування теоретичного матеріалу, розв'язування задач, участь у обговоренні ситуацій);

– тестовий контроль засвоєння теоретичного та практичного матеріалу з теми;

– оцінювання результатів захисту лабораторних робіт;

Підсумкова семестрова оцінка виставляється за результатами поточного контролю. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, вважається таким, який ***має*** академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком, встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

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 практичних та лабораторних занять (вивчення теоретичного матеріалу з теми, попередню підготовку протоколу роботи, підготовку до усного опитування для допуску до заняття (наведені у Методичних рекомендаціях до лабораторних занять)), активно працювати на занятті, брати участь у дискусіях щодо прийнятих рішень при виконанні здобувачами лабораторних робіт.

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 / практичне 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 практичних занять, тестування.

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).

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

Аудиторна робота									**Контрольні заходи**	**Семестровий контроль**
Лабораторні заняття №:								Практичні заняття (8 контрольних точок)	Тестовий контроль	Залік
1*	2	3	4	5	6	7	8	1,2,…,7,8	Т 1-5	
Кількість балів за кожний вид навчальної роботи (мінімум-максимум)										
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5, 3-5, … , 3-5, 3-5	12-20	За рейтингом
24-40								**24-40**	**12-20**	**60-100****

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 на практичних заняттях. Оцінка, яка виставляється за практичне заняття, складається з таких елементів: усне опитування студентів на знання теоретичного матеріалу з теми; уміння професійно обґрунтувати прийняті рішення при розв'язуванні задач; результати самостійних робіт.

При оцінюванні практичного заняття викладач керується узагальненими критеріями, наведеними у таблиці «**Критерії оцінювання навчальних досягнень здобувача вищої освіти**» (мінімальний позитивний бал – 3 бали, максимальний – 5 балів).

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; повнота відповіді та знання.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти.

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 тестового контролю Кожний з тестів, передбачених Робочою програмою, складається із 20 тестових завдань, кожне з яких є рівнозначним.

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

Розподіл балів в залежності від наданих правильних відповідей на тестові завдання

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

На тестування відводиться 30-40 хвилин. Студент проходить тестування в он-лайн режимі у Модульному середовищі для навчання. Також, студент може проходити тестування письмово, записуючи правильні відповіді у талоні відповідей. При отриманні негативної оцінки тест слід перездати до терміну ***наступного*** контролю.

У разі, якщо здобувач вищої освіти виявив рівень знань, 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.

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

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
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

10. Питання для самоконтролю результатів навчання

1. Основні поняття й визначення: атаки, вразливості, політика безпеки, механізми й сервіси безпеки.
2. Взаємозв'язок основних понять безпеки інформаційних систем.
3. Класифікація мережних атак.
4. Модель мережної взаємодії.
5. Модель безпеки інформаційної системи.
6. Основні вимоги до алгоритмів асиметричного шифрування
7. Використання алгоритмів з відкритим ключем для шифрування/дешифрування.
8. Використання алгоритмів з відкритим ключем для створення й перевірка підпису.
9. Модель криптосистеми з відкритим ключем
10. Криптоалгоритм Меркле-Хеллмана
11. Система Idempotent Elements
12. Алгоритм Шаміра
13. Стандарт асиметричного шифрування RSA
14. Стійкість RSA
15. Атака при використанні загального модуля
16. Метод безключового читання RSA
17. Злом RSA на основі підібраного шифртекста
18. Алгоритм Ель-Гамаля
19. Алгоритм Діффі-Хеллмана
20. Криптосистеми на еліптичних кривих. Загальні положення
21. Еліптична крива над полем $GF(p)$
22. Вибір параметрів еліптичних кривих
23. Обмін ключами за схемою Діффі-Хеллмана з використанням еліптичних кривих
24. Протокол Мессі-Омури з використанням еліптичних кривих
25. Шифр Ель-Гамаля на еліптичній кривій
26. Хеш – функції. Загальні положення
27. Хеш – функція MD5
28. Хеш – функція SHA – 1
29. Електронно-цифровий підпис. Загальні положення
30. Алгоритм цифрового підпису RSA
31. Недоліки алгоритму цифрового підпису RSA
32. Атака на підпис RSA в схемі з нотаріусом
33. Електронний підпис на базі шифру Ель-Гамаля
34. Стандарт цифрового підпису DSS. Алгоритм цифрового підпису DSA
35. Стандарт електронного підпису ГОСТ Р 34.10-94
36. Алгоритм електронного підпису ECDSA
37. Використання алгоритмів з відкритим ключем для шифрування/дешифрування.
38. Використання алгоритмів з відкритим ключем для створення й перевірка підпису.
39. Алгоритм RSA.
40. Криптоаналіз RSA.
41. Алгоритм обміну ключа Діфі-Хелмана
42. Хеш-функції. Вимоги до хеш-функцій.
43. Прості хеш-функції
44. Хеш-функції, основані на створенні ланцюжка зашифрованих блоків
45. Хеш-функція MD5. Логіка виконання MD5
46. Структура розширеного повідомлення MD5.
47. Обробка чергового блоку MD5.
48. Алгоритми MD4, MD5. Недоліки, переваги.
49. Хеш - функція SHA-1
50. Обробка чергового блоку SHA-1.
51. Вхідні значення кожного циклу SHA-1
52. Алгоритми SHA-1, MD5. Недоліки, переваги.
53. Хеш-функції SHA-2, SHA-256 ,SHA-384 і SHA-512
54. Коди аутентифікації повідомлень - MAC.
55. MAC на основі алгоритму симетричного шифрування, хеш-функції
56. Алгоритм HMAC
57. Цифровий підпис. Вимоги до цифрового підпису.

11. Навчально-методичне забезпечення

Освітній процес з дисципліни «Програмування криптографічних алгоритмів» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, розміщеною в електронному варіанті в модульному середовищі.

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

Інформаційна та комп'ютерна підтримка: ПК, планшет, смартфон або інший мобільний пристрій, проєктор. Програмне забезпечення: програми Microsoft Visual Studio 2022, доступ до мережі Інтернет, робота з презентаціями.

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

13. Рекомендована література:

Основна

1. Бобала, Ю. Я. Інформаційна безпека/ Ю. Я. Бобала, І. В. Горбатого - Львівська політехніка, 2019. – 640 с.
2. Остапов, С.Е. Технологія захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О. Г. Король. – Х.:Вид. ХНЕУ, 2018р. – 476 с.
3. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. – Хмельницький: ХмНУ, 2020. – 196 с.
4. Лук'янов, Б. В. Комп'ютерний аналіз даних/Б.В.Лук'янов – К. : Академія, 2017. – 345 с.
5. Богуш, В. Основи кіберпростору, кіберзахисту та кібербезпеки./ В. Богуш, В. Бровко, В. Настрадін - Видавництво: Ліра-К., 2021р.- 554 с.
6. Остроухов, В.В. Інформаційна безпека. Підручник / В.В. Остроухов, М.М. Присяжнюк, О. І. Фармагей – К.: Видавництво Ліра-К, 2021р. – 412 с.
7. Ємець, В. Сучасна криптографія. Основні поняття/В.Ємець.- Львів: Бак, 2017р. – 144 с.
8. Stewart J.M., Kinsey D. Network security, firewalls, and VPNs. Burlington : Jones & Bartlett Learning, 2021. - 482 p.
9. Остапов, С. Е. Кібербезпека : сучасні технології захисту. Навчальний посібни. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 778 с.
10. Гончар, С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія./ С.Ф. Гончар. – Київ,2019.–175с.
11. Щур, Н.О. Основи криптології: навч. посібник. / Н.О. Щур, О.А. Покотило – Житомир: Державний університет «Житомирська політехніка», 2021р. - 120 с.
12. Джулій, В.М. Інформаційно-ознакова модель шкідливої інформації в соціальних мережах/ І.В. Муляр, В.М. Джулій, В. М. Пічура, О.О Зацепіна – Вимірювальна та обчислювальна техніка в технологічних процесах № 3 (2022)-73–78с.
13. Джулій, В.М. Модель визначення актуальних загроз безпеки конфіденційних даних в розподіленій інформаційній системі / В.М. Джулій, М.В. Димбовський, І.В. Муляр // Збірник наукових праць ВІКНУ ім. Т. Шевченка. – К.: ВІКНУ, 2023. –№ 80. – С.78
14. Джулій, В.М. Дослідження актуальних загроз безпеки конфіденційної інформації/М.В. Димбовський, В.М. Джулій - Військова освіта і наука: сьогодення та майбутнє: зб. тез доповідей XIX Міжнародної науково-практичної конференції, м. Київ, 10 листопада 2023 р. Київ: Військовий інститут Київського національного університету імені Тараса Шевченка, 2023. – С. 33.
15. Джулій, В.М. Метод класифікації додатків інтернет - трафіка комп'ютерних мереж в умовах невизначеності / В.М. Джулій, Л.В. Солодєєва, О.В. Мірошніченко, // Збірник наукових праць ВІКНУ ім. Т. Шевченка. – К.: ВІКНУ, 2022. –№74. – С. 73-82.
16. Вербіцкий О. В. Вступ до криптології./ О. В. Вербіцкий - Львів: ВНТА, 2017. –247 с.
17. Лєнков С. В. Динамічні показники оцінки рівня функціональної безпеки інформаційної системи / С. В. Лєнков, В. М. Джулій, І. В. Муляр // Сучасна спеціальна техніка. - 2016. - № 2. - С. 59-67.
18. Джулій В. М. Моделі та алгоритми виявлення атак в бездротових мережах передачі даних / В. М. Джулій, О. С. Лєнков, Л. О. Ряба // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Київ : ВІКНУ, 2018. – Вип. 59. – С. 76-87.
19. Метод передачі прихованої інформації без спотворення растрового зображення / С. В. Лєнков, В. М. Джулій, О. В. Мірошніченко, Б. О. Бойко // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Київ : ВІКНУ, 2017. – Вип. 58. – С. 114-123.

Додаткова

20. Лісовська, Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
21. Бем, М. В. Стандарти захисту персональних даних в соціальній сфері. / М. В.Бем, І. М. Городиський - Львів:, 2018р. - 110 с.
22. Бурячок, В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко – К. : ДУТ-КНУ, 2017. – 178 с.
23. Гошубєв, О.В. Програмно-технічні засоби захисту даних від комп'ютерних злочинів / О. В. Гошубєв– Запоріжжя : «Павел», 2018. – 145с.
24. Горбулін, П.В. Проблеми захисту інформаційного простору України / М.М. Баченок, П.В. Горбулін – К.: Інтертехнологія, 2019. – 138 с.
25. Хорошко, В.О. Захист систем електронних комунікацій: навч. посіб. / В.О. Хорошко, О.В. Криворучко, М.М. Браіловський - Київ., 2019р. – 164 с.
26. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ.ун-т внутріш. справ, 2020. – 128 с.
27. Andress J. Foundations of information security: a straightforward introduction. San Francisco: No Starch Press, 2019.- 222 p.
28. Кобозева, А.А. Аналіз захищеності інформаційних систем: підр./ А.А.Кобозева, І.О. Мачалін, В.О.Хорошко – Київ: ДУІКТ, 2019. – 316
29. OPWNAI: Cybercriminals Starting to Use ChatGPT, January 6, 2023 [Електронний ресурс] Режим доступу до ресурсу: https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-usechatgpt

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL : https://msn.khnu.km.ua/course/view.php?id=5908
2. Електронна бібліотека ХНУ. URL: http://library.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://elar.khmnu.edu.ua/home

ПРОГРАМУВАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Тип дисципліни	Вибіркова
Рівень вищої освіти	Перший (бакалаврський)
Мова викладання	Українська
Семестр	-
Кредити ЄКТС	8,0
Форми навчання, для яких викладається дисципліна	Очна (денна)

Результати навчання. Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати* знання алгоритмів захисту інформації і технологій їх програмної реалізації у практичних ситуаціях, адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; використовувати програмні та програмно-апаратні комплекси засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах, *обирати* відповідну технологію програмування і *виконувати* аналіз специфікації задач, *вирішувати* завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень, *забезпечувати* функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, *вирішувати* задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних методів та засобів криптографічного захисту інформації, *виконувати* впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; *використовувати* інформаційно-комунікаційні технології, сучасні методи і моделі інформаційної безпеки та/або кібербезпеки, *застосовувати* теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

Зміст навчальної дисципліни. Методи і моделі інформаційної безпеки. Методи та засоби криптографічного захисту інформації. Алгоритми реалізації основних методів захисту інформації з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників. Спеціальне програмне забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах Керування ризиками й побудова систем мережної безпеки. Методологія побудови системи інформаційної безпеки підприємства.

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*:* Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій та методів навчання, зокрема: лекції (з використанням методів візуалізації, проблемного й інтерактивного навчання, мотиваційних прийомів, інформаційно-комунікаційних технологій); практичні заняття (з використанням інструктування, демонстрування, розв'язування типових і прикладних задач, аналізу кейсів, ситуаційних завдань, елементів дискусії тощо); самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання практичних робіт, поточного та підсумкового контролю, виконання індивідуальних та домашніх завдань), з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

Форми оцінювання результатів навчання*:* Поточний контроль здійснюється під час аудиторних практичних та 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 роботи на практичних заняттях (опитування теоретичного матеріалу, розв'язування задач, участь у обговоренні ситуацій); тестовий контроль засвоєння теоретичного та практичного матеріалу з теми; оцінювання результатів захисту лабораторних робіт;

Вид семестрового контролю: залік.

Навчальні ресурси:

1. Бобала, Ю. Я. Інформаційна безпека/ Ю. Я. Бобала, І. В. Горбатого - Львівська політехніка, 2019. – 640 с.
2. Остапов, С.Е. Технологія захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О. Г. Король. – Х.:Вид. ХНЕУ, 2018р. – 476 с.
3. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. – Хмельницький: ХмНУ, 2020. – 196 с.
4. Богуш, В. Основи кіберпростору, кіберзахисту та кібербезпеки./ В. Богуш, В. Бровко, В. Настрадін - Видавництво: Ліра-К., 2021р.- 554 с.
5. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ.ун-т внутріш. справ, 2020. – 128 с.
6. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/.
7. Електронна бібліотека ХНУ. Доступ до ресурсу: http://library.khmnu.edu.ua/.

Викладач: канд. техн. наук, доцент Володимир ДЖУЛІЙ.
викладач Олена ПИРЧ