ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету ІТ
_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
«31» 08 2024 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Програмування криптографічних алгоритмів

Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека
Рівень вищої освіти	Перший бакалаврський
Освітньо-професійна програма	Кібербезпека
Обсяг дисципліни	8 кредитів ЄКТС
Шифр дисципліни	ВД5877
Мова навчання	Українська
Статус дисципліни	Вибіркова
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Очна (денна)	-	-	8	240	90	36	36	18		150			+	

Робоча програма складена _____ канд.техн.наук, доцт Володимир ДЖУЛІЙ
Підпис(и) автора(ів) Ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 30.08.2024 № 1 Зав. кафедри _____ 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 2024

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	Денна

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.

Пререквізити: -.

Кореквізити: -.

Запланована навчальна діяльність: всього 240 год., у т.ч. лекцій – 36 год., лабораторних занять – 36 год., практичних занять – 18 год., самостійної роботи – 150 год.

Форми (методи) навчання: пояснювально-ілюстративні, продуктивні та репродуктивні, практичні, проблемні, тренінгові, моделювання, застосування інформаційно-комп'ютерних технологій.

Форми оцінювання результатів навчання: усне опитування, тестування, захист лабораторних робіт, вирішення практичних завдань, підсумковий контрольний захід (семестровий контроль).

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 університету. Доступ до ресурсу: http://library.khmnu.edu.ua/.

Викладач: канд. техн. наук, доцент Джулій В.М.

ВСТУП

Дисципліна "Програмування криптографічних алгоритмів" є етапом підготовки до самостійної практичної діяльності з розробки і екплуатації безпечних програмних додатків і тому займає провідне місце у підготовці бакалаврів з кібербезпеки.

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. Забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності „Кібербезпека та захист інформації":

компетентності:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

результати навчання:

ПРН 1(5). Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН 2(14). Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень.

ПРН 3(19). Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПРН 4(47). Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних методів та засобів криптографічного захисту інформації.

ПРН 5. Обирати відповідну технологію програмування, виконати аналіз специфікації задач.

ПРН 6. Використовувати прикладні системи програмування, *розроблятиме* складні програмні комплекси з функціями захисту даних (із застосуванням мови C# тощо);

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.

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин, відведених на:			
	лекції	лабораторні роботи	практичні роботи	самостійну роботу
Тема 1. Основні поняття інформаційної безпеки. Класифікація методів та алгоритмів захисту інформації. Основи криптографії та криптоаналізу.	8	8	8	24
Тема 2. Ідентифікація й аутентифікація. Поняття протоколу ідентифікації. Ідентифікуюча інформація.	4	8	2	28
Тема 3. Криптографія з відкритим ключем. Алгоритми асиметричного шифрування. Хеш – функції і аутентифікація повідомлень	10	8	4	28
Тема 4. Цифрова підпис. Стандарт цифрового підпису. Протоколи аутентифікації.	10	2	2	34
Тема 5. Керування ризиками й побудова систем мережної безпеки	4	10	2	36
Разом:	**36**	**36**	**18**	**150**

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.		
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.		
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		
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	**Алгоритм MD4. Посилення алгоритму в MD5**. **Хеш-функція SHA-1**. Хеш-функції й аутентифікація повідомлень. Коди аутентифікації повідомлень – MAC. Літ.:[1] с.167-185; [2] с.155-167;	2
11	**Хеш-функції.**. Хеш-функції SHA-2, SHA-384, SHA-512, SHA-1024, Літ.:[1] с.167-185; [2] с.155-167;	
Тема 4. Цифрова підпис. Стандарт цифрового підпису. Протоколи аутентифікації.		
12	**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
13	**Алгоритми обміну ключів і протоколи аутентифікації**. Протоколи аутентифікації. Протокол Нідхема й Шредера. Протокол Деннінга. Літ.:[1] с.209-424; [2] с.162-171;	2
14	**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
15	**Технології аутентифікації.** Протокол аутентифікації з використанням квитка. Аутентификация, авторизація й адміністрування дій користувачів. Використання шифрування з відкритим ключем. Літ.:[1] с.443-543;	2
16	**Протокол аутентифікації з використанням аутентифікаційного сервера.** Одностороння аутентифікація.Протокол аутентифікації з використанням KDC. Використання симетричного шифрування. Використання шифрування з відкритим ключем Літ.:[1] с.443-543; [2] с.171-205;	2
Тема 5. Керування ризиками й побудова систем мережної безпеки		
17	**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
18	**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:	**36**

Перелік 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
9	Підсумкове заняття	4
	Разом за семестр:	**36**

Перелік 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	2
9	Підсумкове заняття	2
	Разом за семестр:	**18**

Зміст самостійної (індивідуальної) роботи

Об'єм самостійної роботи становить 150 годин. Він включає опрацювання лекційного матеріалу, підготовку до виконання лабораторних робіт і їх захисту, підготовку до поточного контролю, а також самостійну роботу студентів.

Номер тижня	Теми самостійної роботи	Кількість годин
1	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №1	8
2	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №1	8
3	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №2	8
4	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №2	8
5	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №3	8
6	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 3.	8
7	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №4.	8
8	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №4.	8
9	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи № 5	8
10	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 5	8
11	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи № 6	8
12	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 6	8
13	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи № 7	8
14	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної №7	8
15	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи № 8	8
16	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 8	10
17	Опрацювання лекційного матеріалу. Підготовка до тестування	10
18	Опрацювання лекційного матеріалу. Підготовка до підсумкового заняття.	10
	Разом за семестр:	**150**

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів, зокрема: лекції (з використанням пояснювально-ілюстративних, репродуктивних, інтерактивних методів і візуалізації); практичні заняття (з використанням тренінгових та практичних методів); лабораторні роботи (з використанням продуктивних, практичних, проблемних, тренігових методів та моделювання); використання сучасних інформаційно-комп'ютерних технологій (CryptoAPI тощо).

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: виконання частини лабораторних робіт передбачає роботу у малих групах з призначенням тім-лідера, що сприяє розвитку лідерських якостей у студентів, здатності до спілкування і організації командної роботи над спільними задачами, а змінюваність складу робочих груп між лабораторними роботами сприяє розвитку навичок адаптованості, гнучкості, комунікативності і оперативного налагоджування міжособистісних відносин в різних колективах; інтерактивне спілкування з проблемних питань під час лекцій, прилюдні захисти лабораторних робіт і виступи під час практичних занять з обґрунтуванням прийнятих рішень щодо вибору методів рішення завдань в діалозі з викладачем і групою сприяють формуванню і удосконаленню вмінь публічних виступів, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики; адаптованість, вміння користуватися інтернет-ресурсами та іншими джерелами інформації, синтезувати та критично осмислювати інформацію з різних джерел передбачені специфікою дисципліни, що передбачає рішення проблемних завдань із застосуванням творчих підходів в синтезі і аналізі програмних рішень і орієнтацію на роботу з постійно оновлюваними технологіями програмування та захисту інформаційних ресурсів; обмежений час на виконання лабораторних робіт, практичних і тестових завдань, чітко визначені терміни проходження контрольних точок і відпрацювання заборгованостей сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту).

При вивченні дисципліни можуть бути зараховані результати навчання, здобуті у неформальній освіті.

МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час практичних та лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни.

При цьому використовуються такі методи поточного контролю:

- усне опитування;
- захист лабораторної роботи;
- вирішення практичних завдань;
- тестування.

Семестровий контроль проводиться у формі заліку. При виведенні підсумкової семестрової оцінки враховуються результати поточного контролю.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами

Аудиторна робота			**Контрольні заходи**	**Підсумковий контрольний захід**
Лабораторні роботи №:		Практичні роботи №:	Тестовий контроль:	Семестровий контроль (залік)
1 - 8		1 - 8	Т 1-5	Залік за рейтингом
ВК:	0,4	0,4	0,2	

Умовні позначення: Т – тема дисципліни; ВК – ваговий коефіцієнт;

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторне заняття, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення; вільне володіння студентом спеціальною термінологією і уміння фахово обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторне заняття викладач оголошує одразу після захисту звіту з лабораторної роботи і проставляє в електронний журнал дисципліни.

Оцінювання практичних занять. Оцінка, яка виставляється за практичне заняття, складається з таких елементів: здатність обрати оптимальний спосіб рішення завдання і обґрунтувати зроблений вибір; правильність та самостійність розв'язування задач, якість отримуваних результатів; вільне володіння студентом спеціальною термінологією і застосовуваними методами дисципліни; уміння фахово обґрунтувати прийняті конструктивні та аналітичні рішення.

Оцінку, отриману на практичному занятті, викладач оголошує студенту одразу після його відповіді і проставляє в електронний журнал дисципліни.

Впродовж семестру студент має отримати на практичних заняттях щонайменше три позитивні оцінки, щоб виконати програму дисципліни.

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

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	1-5	6-12	13–18	19-20
Оцінка за 4-ри бальною шкалою	2	3	4	5

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

Тестування студент може також пройти і в он-лайн режимі в модульному середовищі для навчання.

Оцінку за тестування викладач проставляє в електронний журнал дисципліни.

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

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	**Узагальнений критерій**
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві - три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка „задовільно".

Студент, який набрав позитивний середньозважений бал за поточну роботу, вважається невстигаючим.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	Інституційна інтервальна шкала балів	Інституційна оцінка, критерії оцінювання	
A	4,75–5,00	5	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4	***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4	***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3	***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3	***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2	***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ЗДОБУТИХ СТУДЕНТАМИ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. 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.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

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

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. Бачено к, 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

ІНФОРМАЦІЙНІ РЕСУРСИ

Електронний університет:

1. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/.
2. Електронна бібліотека університету. Доступ до ресурсу: http://library.khmnu.edu.ua/.