ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки

ЗАТВЕРДЖУЮ
Декан ФІТ
Тетяна ГОВОРУЩЕНКО
«31» серпня 2024 р.

СИЛАБУС

Навчальна дисципліна: «*Програмування криптографічних алгоритмів*»

Освітньо-професійна програма: «Кібербезпека та захист інформації»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Джулій Володимир Миколайович
Профайл викладач(ів)	https://kb.khmnu.edu.ua/dzhulij-volodymyr-mykolajovych/
E-mail викладача(ів)	dzhuliivm@khmnu.edu.ua
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/course/view.php?id=5908
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://zoom.us/j/3576738561 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр IV (зимово-весняний)
Консультації	Очні: згідно графіку консультацій Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

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
ОД	-	-	8	240	90	36	36	18	-	150	-	-	+	-

Анотація дисципліни

Дисципліна «Програмування криптографічних алгоритмів» є вибірковою, викладається для студентів очної денної форми навчання, рекомендована для здобувачів вищої освіти за освітньо-професійною програмою «Кібербезпека» першого (бакалаврського) рівня. При викладанні дисципліни використовуються наступні форми (методи) навчання: словесні та наочні (лекції); практичні та частково-пошукові (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Пререквізити –.

Кореквізити –.

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":

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, *розробляти* 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.

Тематичний і календарний план вивчення дисципліни на IV семестр (18 тижнів)

Номер тижня	Номер теми	Тема лекції	Тема практичної роботи	Тема лабораторної роботи	Самостійна робота студента		
					Зміст	Години	Література
1	2	3	4	5	6	7	8
1	1	Основні поняття й визначення: атаки, вразливості, політика безпеки, механізми й сервіси безпеки. Модель мережної безпеки.	**ПЗ1.** Наскрізна практична робота: захист програмного забезпечення від нелегального копіювання.	**ЛР1.** Методи генерації псевдовипадкових чисел.	Опрацювання лекційного матеріалу. Підготовка до виконання ЛР1.	8	[1 с.133-145; 2 с.148-155]
2	1	Класифікація мережних атак. Модель мережної взаємодії. Сервіси безпеки. Модель безпеки інформаційної системи			Отримання завдання на індивідуальну роботу під керівництвом викладача.	8	[1 с.133-145; 2 с.148-155]
3	1	Криптографія з відкритим ключем. Основні вимоги до алгоритмів асиметричного шифрування. Алгоритм RSA.	**ПЗ2.** Бібліотека класів (DLL). Генератор паролів	**ЛР2.** Потокові алгоритми шифрування.	Опрацювання лекційного матеріалу. підготовка до захисту ЛР1. захист ЛР1.	8	[1 с.133-145; 2 с.148-155]
4	1	Алгоритм обміну ключа Діфі-Хелмана. Цифровий (електронний) підпис на основі криптосистеми RSA.			Опрацювання лекційного матеріалу. Підготовка до виконання ЛР2.	8	[1 с.133-145; 2 с.148-155]
5	2	Основні поняття й визначення: атаки, вразливості, політика безпеки, механізми й сервіси безпеки. Модель мережної безпеки.	**ПЗ3.** Реалізувати власний алгоритм шифрування	**ЛР3.** Блочні шифри.	Робота над індивідуальним завданням. Захист ЛР2.	8	[1 с.151-167; 2 с.155-157]
6	2	Хеш-функції, основані на створенні ланцюжка зашифрованих блоків. Хеш-функція MD5.			Опрацювання лекційного матеріалу. Підготовка до захисту ЛР3. Захист ЛР3.	8	[1 с.167-185; 2 с.155-157]
7	2	Алгоритм MD4. Посилення алгоритму в MD5. Хеш-функції й аутентифікація повідомлень.	**ПЗ4.** Алгоритм RSA. Хеш-функція. Програмна реалізація.	**Хеш функції**. Програмна реалізація	Робота над індивідуальним завданням. Підготовка до виконання ЛР4.	8	[1 с.167-185; 2 с.155-157]
8	2	Хеш-функція SHA-1. Коди аутентифікації повідомлень – MAC.			Опрацювання лекційного матеріалу. Захисту ЛР4.	8	[1 с.185-199; 2 с.157-162]
9	3	Цифровий підпис. Вимоги до цифрового	**ПЗ5.** Робота з реєстром. Клас	**ЛР5.** Електронний	Робота над індивідуальни	8	[1 с.185-199;

		підпису. Пряма й арбітражна цифрові підписи.	Registry. Технологія WMI.	цифровий підпис RSA.	м завданням Підготовка до захисту ЛР5		2 с.157-162]
10	3	Стандарт цифрового підпису DSS. Стандарт цифрового підпису ГОСТ 3410/			Опрацювання лекційного матеріалу. Захист ЛР5.	8	[1 с.209-424; 2 с.162-171]
11	4	Алгоритми обміну ключів і протоколи аутентифікації. Алгоритми розподілу ключів з використанням третьої довіреної сторони.	**ПЗ6.** Робота з мережами в C# і .NET.	**ЛР6.** Криптографія на еліптичних кривих.	Робота над індивідуальним завданням. Підготовка до виконання ЛР6.	8	[1 с.209-424; 2 с.162-171]
12	4	Протоколи аутентифікації. Протокол Нідхема й Шредера. Протокол Деннінга.			Опрацювання лекційного матеріалу. Захист ЛР6.	8	[1 с.443-543; 2 с.171-205]
13	4	Технології аутентифікації. Аутентифікація, авторизація й адміністрування дій користувачів.	**ПЗ7.** Програмна реалізація сервера. Налагодження взаємодії клієнтської програми та сервера	**ЛР7.** Реалізувати обмін ключами з використанням еліптичних кривих,	Робота над індивідуальним завданням. Підготовка до захисту ЛР7	8	[1 с.443-543; 2 с.171-205]
14	4	Протокол аутентифікації з використанням квитка. Використання шифрування з відкритим ключем.			Опрацювання лекційного матеріалу. Захист ЛР7.	8	[1 с.443-543; 2 с.171-205]
15	4	Протокол аутентифікації з використанням аутентифікаційного сервера. Протокол аутентифікації з використанням KDC.	**ПЗ8.** Реєстрація нового клієнта. Клас Hesh на сервері.	**ЛР8.** Реалізувати електронно-цифрову підпис з використанням еліптичних кривих	Робота над індивідуальним завданням Підготовка до захисту ЛР8	8	[1 с.443-543; 2 с.171-205]
16	4	Одностороння аутентифікація. Використання симетричного шифрування. Використання шифрування з відкритим ключем.			Опрацювання лекційного матеріалу. Захист ЛР8. Підготовка до захисту ЛР9.	10	[2 с.531-548; 8 с.269-273; 9 с.605-706]
17	5	Керування ризиками й побудова систем мережної безпеки. Аналіз і керування ризиками. Основні поняття й визначення. Технологія аналізу й керування ризиками. Засоби автоматизації оцінки інформаційних ризиків.			Опрацювання лекційного матеріалу. Захист ЛР9	10	[2 с.531-548; 8 с.269-273; 9 с.605-706]
18	5		**Підсумкове заняття**	**Підсумкове заняття**	Робота над індивідуальним завданням. Захист ного завдання.	10	[2 с.531-548; 8 с.269-273; 9 с.605-706]

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 іспиту. При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контрольного заходу.

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 у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

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

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

Співвідношення 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. 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

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/.