ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки

ЗАТВЕРДЖУЮ
Декан ФІТ
_____ Тетяна ГОВОРУЩЕНКО
«_31_» ____08_____ 2024 р.

СИЛАБУС
Навчальна дисципліна: "*Прикладна криптологія*"

Освітньо-професійна програма: «Кібербезпека та захист інформації»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Тітова Віра Юріївна Петрушак Володимир Степанович Анікін Володимир Андрійович
Профайл викладач(ів)	https://kb.khmnu.edu.ua/sklad-kafedry/
E-mail викладача(ів)	v.titova231@gmail.com anikin_volodymyr@khmnu.edu.ua
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=6453
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us05web.zoom.us/j/521227760 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр IV (зимово-весняний) 2025-2026, семестр V (осінньо-зимовий)
Консультації	Очні: згідно графіку консультацій Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
ОД	2	4	4	120	54	18	36	-	-	66	-	-	-	+
ОД	3	5	5	150	51	17	34	-	-	99	-	-	-	+
Разом:			**9**	**270**	**105**	**35**	**70**	**-**	**-**	**165**	**-**	**-**	**-**	**2**

Анотація дисципліни

Дисципліна викладається для студентів денної форми навчання спеціальності «Кібербезпека та захист інформації. 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 – математичні основи захисту інформації; теорія інформації та кодування.

Кореквізити – проєктно-технологічна практика; компонентна база і схемотехніка систем захисту.

Мета і завдання дисципліни

Метою викладання навчальної дисципліни є формування у майбутніх спеціалістів умінь та компетенцій для ефективного застосування методів та засобів криптографічного захисту інформації на об'єктах інформаційної діяльності; розвиток у студентів фахового стилю мислення; надання глибоких та міцних знань з питань криптографічного захисту інформації в умовах широкого використання сучасних інформаційних технологій.

Предметом дисципліни є методи та засоби криптографічного захисту інформації; сучасне програмно-апаратне забезпечення криптографічного захисту інформаційно-комунікаційних технологій та систем.

Завданням дисципліни є забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до освітньо-професійної програми підготовки бакалаврів зі спеціальності «Кібербезпека та захист інформації»:

***компетентності*:**

ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

результати навчання:

ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

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

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

ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах

Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати* теорії та методи криптографічного захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; *вирішувати* задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних методів та засобів криптографічного захисту інформації; *виконувати* впровадження та підтримку компонентів криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; *адаптуватися* в умовах частої зміни технологій професійної діяльності та *прогнозувати* кінцевий результат при вирішенні практичних задач криптографічного захисту інформації.

Тематичний і календарний план вивчення дисципліни (семестр IV)

№ тижня	Тема лекції*	Тема лаб. роботи **	Самостійна роботи		
			Зміст	Год.	Література
1	**Тема 1. Введення в криптологію**	**ЛР1**. Шифри стовпцевої перестановки та подвійної перестановки	Опрацювання теоретичного матеріалу лекції №1.	3	[3] с. 14-36
2	-	**ЛР1.** Підгрупа 2.	Підготовка до виконання лабораторної роботи №1	4	[2] с. 131-140; [3] с. 42-89
3	**Тема 2. Класичні шифри (частина 1)**	**ЛР2.** Шифри простої заміни	Опрацювання теоретичного матеріалу лекції №2.	3	[2] с. 131-140; [3] с. 42-89
4	-	**ЛР2.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2.	4	[2] с. 140-147; [3] с. 89-101
5	**Тема 2. Класичні шифри (частина 2)**	**ЛР3.** Шифр Цезаря	Опрацювання теоретичного матеріалу лекції №3.	3	[2] с. 140-147; [3] с. 89-101
6	-	**ЛР3.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3.	4	[2] с. 140-147; [3] с. 89-101
7	**Тема 3. Симетричні криптосистеми** Потокові та блочні симетричні шифри	**ЛР4.** Шифр Віженера	Опрацювання теоретичного матеріалу лекції №4.	3	[1] с. 47-60; [2] с. 147-158; [3] с. 101-127, 148-172
8	-	**ЛР4.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4.	4	[2] с. 140-147; [3] с. 89-101
9	**Тема 3. Симетричні криптосистеми** Міжнародні стандарти блокового симетричного шифрування (частина 1)	**ЛР5.** Шифр XOR (шифр одноразового блокнота)	Опрацювання теоретичного матеріалу лекції №5.	3	[2] с. 158-169; [3] с. 172-215, 228-264

10	-	**ЛР5.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №4. Підготовка до виконання лабораторної роботи №5.	4	[2] с. 140-147; [3] с. 89-101
11	**Тема 3. Симетричні криптосистеми** Міжнародні стандарти блокового симетричного шифрування (частина 2)	**ЛР6.** Шифри DES та 3DES	Опрацювання теоретичного матеріалу лекції №6.	3	[2] с. 171-179; [3] с. 310-370
12	-	**ЛР6.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6.	4	[2] с. 158-169; [3] с. 172-215, 228-264
13	**Тема 3. Симетричні криптосистеми** Вітчизняні стандарти блокового симетричного шифрування	**ЛР7.** Шифр AES	Опрацювання теоретичного матеріалу лекції №7.	3	[2] с. 169-171, 179-191; [3] с. 270-310
14	-	**ЛР7.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7.	5	[2] с. 171-179; [3] с. 310-370
15	**Тема 4. Асиметричні криптографічні системи шифрування (частина 1)**	**ЛР8.** Шифр RSA	Опрацювання теоретичного матеріалу лекції №8.	3	[3] с. 386-418
16	-	**ЛР8.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8.	5	[3] с. 386-418
17	**Тема 4. Асиметричні криптографічні системи шифрування (частина 2)**	Підсумкове заняття **Контрольна робота**	Опрацювання теоретичного матеріалу лекції №9. Підготовка до контрольної роботи за пройденим матеріалом.	3	[3] с. 386-418
18	-	Підсумкове заняття **Контрольна робота** Підгрупа 2.	Підготовка до захисту лабораторної роботи №8.	5	[3] с. 386-418

*** лекції проводяться по 2 години раз на два тижні;**
**** лабораторні проводяться по 4 години раз в два тижні.**

Тематичний і календарний план вивчення дисципліни (семестр V)

№ тижня	Тема лекції*	Тема лаб. роботи **	Самостійна роботи		
			Зміст	Год.	Література
1	**Тема 1. Елементи криптоаналізу (частина 1)**	**ЛР1**. Частотний криптоаналіз шифру Цезаря та заміни	Опрацювання теоретичного матеріалу лекції №1.	3	[2] с. 220-247; [4] с. 6-29, 46-50
2	-	**ЛР1.** Підгрупа 2.	Підготовка до виконання лабораторної роботи №1	4	[2] с. 220-247; [4] с. 6-29, 46-50
3	**Тема 1. Елементи криптоаналізу (частина 2)**	**ЛР2.** Лінійний криптоаналіз блочного симетричного шифру	Опрацювання теоретичного матеріалу лекції №2.	3	[3] с. 127-135, 215-228, 264-270, 370-386, 418-430
4	-	**ЛР2.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2.	4	[3] с. 127-135, 215-228, 264-270, 370-386, 418-430
5	**Тема 1. Елементи криптоаналізу (частина 3)**	**ЛР3.** Диференціальний криптоаналіз блочного симетричного шифру	Опрацювання теоретичного матеріалу лекції №3.	3	[3] с. 127-135, 215-228, 264-270, 370-386, 418-430
6	-	**ЛР3.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3.	4	[3] с. 127-135, 215-228, 264-270, 370-386, 418-430
7	**Тема 2. Автентифікація та хешування** Основи теорії автентичності	**ЛР4.** Оцінювання стійкості паролів	Опрацювання теоретичного матеріалу лекції №4.	3	[2] с. 272-284
8	-	**ЛР4.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4.	4	[2] с. 272-284
9	**Тема 2. Автентифікація та хешування** Криптографічні хеш-функції (частина 1)	**ЛР5.** Хеш-функції	Опрацювання теоретичного матеріалу лекції №5.	3	[2] с. 284-296
10	-	**ЛР5.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №4. Підготовка до виконання лабораторної роботи №5.	4	[2] с. 284-296

11	**Тема 2. Автентифікація та хешування** Криптографічні хеш-функції (частина 2)	**ЛР6.** Розмежування повноважень на основі парольної аутентифікації	Опрацювання теоретичного матеріалу лекції №6.	3	[2] с. 296-308
12	-	**ЛР6.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6.	4	[2] с. 284-296
13	**Тема3. Цифрові підписи**	**ЛР7.** Цифровий підпис RSA та Ель-Гамаля	Опрацювання теоретичного матеріалу лекції №7.	3	[1] с. 117-129
14	-	**ЛР7.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7.	5	[1] с. 117-129
15	**Тема 4. Стеганографія (частина 1)**	**ЛР8.** Приховування інформації у текстові та графічні файли	Опрацювання теоретичного матеріалу лекції №8.	3	[2] с. 251-260
16	-	**ЛР8.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8.	5	[2] с. 251-272
17	**Тема 4. Стеганографія (частина 2)**	Підсумкове заняття **Контрольна робота**	Опрацювання теоретичного матеріалу лекції №9. Підготовка до контрольної роботи за пройденим матеріалом. Підготовка до захисту лабораторної роботи №8.	3	[2] с. 260-272

ПОЛІТИКА ДИСЦИПЛІНИ

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції і лабораторні заняття згідно з розкладом, не запізнюватися на заняття, вчасно виконувати та здавати лабораторні роботи. Термін виконання лабораторної роботи вважається своєчасним, якщо студент здав/захистив її на поточному або наступному за ним занятті. За несвоєчасний захист лабораторної роботи з набраної студентом суми балів вираховується один бал. Пропущене з поважної причини лабораторне заняття студент повинен відпрацювати у встановлений викладачем термін.

Виконуючи усі навчальні завдання з дисципліни, студент має дотримуватися політики доброчесності. У разі наявності плагіату він отримує незадовільну оцінку і має виконати завдання за новою темою.

Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок визнання та перезарахування результатів навчання здобувачів вищої освіти у ХНУ.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». 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 (IV семестр)

	Аудиторна робота	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Контрольна робота	Семестровий контроль (іспит)
Тема	2-4	1-4	1-4
Ваговий коефіцієнт	0,4	0,2	0,4

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами (V семестр)

	Аудиторна робота	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Контрольна робота	Семестровий контроль (іспит)
Тема	1-4	1-4	1-4
Ваговий коефіцієнт	0,4	0,2	0,4

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторну роботу, складається з таких елементів: оцінка, отримана за здачу відповідної за номером та темою практики; знання теоретичного матеріалу з теми; якість оформлення звіту; вільне володіння студентом спеціальною термінологією і уміння професійно 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 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 лабораторну роботу викладач оголошує одразу після захисту звіту і проставляє в електронний журнал дисципліни.

Оцінювання контрольних робіт. Контрольна робота складається з двох теоретичних питань та однієї задачі за темами практичних занять. Оцінювання здійснюється за чотирибальною шкалою.

Оцінку «відмінно» отримує студент який дав повну письмову відповідь на теоретичні питання та правильно вирішив задачу.

Оцінку «добре» отримує студент, який дав правильну відповідь на теоретичні питання та правильно вирішив задачу, але у відповіді присутні дві-три несуттєві помилки.

Оцінку «задовільно» отримує студент, який дав часткову відповідь на теоретичні питання або припустився помилок при вирішення задачі.

Оцінку «незадовільно» отримує студент, який не дав відповіді на теоретичні питання або не зміг вирішити задачу.

Оцінку за контрольну роботу викладач проставляє в електронний журнал дисципліни не пізніше ніж через десять днів після проведення контрольного заходу.

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з двох теоретичних питань і задачі. Під час іспиту за наданими відповідями і рішеннями (розв'язками) виконується оцінювання рівня засвоєння студентом матеріалу дисципліни.

Оцінка за підсумковий контрольний захід проставляється викладачем в електронний журнал дисципліни в день здачі іспиту і враховується в автоматизованому режимі при визначенні підсумкової семестрової оцінки студента з дисципліни за інституційною шкалою і шкалою ЄКТС

Засвоєння студентом 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 вітчизняної 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. Роль криптографічних протоколів у задачі забезпечення інформаційної безпеки.
2. Основні визначення, використовувані в криптології.
3. Узагальнена схема криптографічної системи.
4. Основи теорії засекреченого зв'язку К. Шеннона.
5. Шифри простої заміни
6. Гомофонний шифр заміни
7. Поліграмні шифри
8. Поліалфавітні шифри
9. Шифри перестановки
10. Багаторазове шифрування
11. Роторні шифрувальні машини
12. Афінні шифри.
13. Шифр гамування
14. Потокові симетричні шифри (A5, RC4, STRUMOK).
15. Синхронні та самосинхронізовані потокові шифри.
16. Блокові симетричні шифри (RC2, RC5, SAFER, FEAL, Blowfish, мережа Фейстеля).
17. Методи компонування сучасних блокових симетричних шифрів.
18. Стандарт DES. Структура алгоритму шифрування даних.
19. Стандарт DES. Режими виконання алгоритму.
20. Симетричний алгоритм IDEA. Структура алгоритму шифрування даних.
21. Симетричний алгоритм IDEA. Безпека та вразливість ключів.
22. Стандарт AES (Rijndael). Структура алгоритму та раундів.
23. Стандарт AES (Rijndael). Алгоритм розгортання ключа для шифрування даних.
24. Стандарт AES (Rijndael). Відмінності шифрування та розширування.
25. Стандарт ДСТУ 28147:2009. Шифрування даних у режимі простої заміни.
26. Стандарт ДСТУ 28147:2009. Шифрування даних у режимі гамування та зі зворотним зв’язком.
27. Стандарт ДСТУ 28147:2009. Шифрування даних у режимі утворення імітовставки.
28. Стандарт блокового симетричного шифрування ДСТУ 7624:2014 «Калина»
29. Основні визначення випадкової послідовності та вимоги до них.
30. Методи і засоби перевірки на випадковість.
31. Конгруентні генератори псевдовипадкових чисел.
32. Генератор Фібоначі.
33. Генератор псевдовипадкових чисел на основі алгоритму BBS.
34. Генератори псевдовипадкових чисел на основі регістрів зсуву зі зворотним зв'язком.
35. Криптографічна система Діффі–Хеллмана
36. Криптографічна система RSA
37. Криптографічна система Ель-Гамаля
38. Типи розкриття
39. Силові методи криптоаналізу
40. Криптоаналіз за побічними каналами
41. Криптоаналіз класичних шифрів.
42. Диференціальний криптографічний аналіз.
43. Лінійний криптографічний аналіз.
44. Властивості симетричності та вразливі ключі.
45. Атака “Квадрат”.
46. Атака методом інтерполяцій.
47. Атака еквівалентних ключів.
48. Методи зламу на дискретному логарифмуванні.
49. Метод “крок немовляти, крок велетня”.
50. Ідентифікація та автентифікація об’єктів
51. Задачі автентифікації у криптографічному захисті інформації

52. Парольна автентифікація. Методи формування стійких паролів
53. Поняття безумовно безпечних кодів автентифікації, теорія Симонсона.
54. Алгоритм MD5
55. Алгоритм SHA
56. Алгоритм SHA3
57. Застосування функції хешування в криптографії
58. Хеш-функції, що використовують симетричні блокові алгоритми
59. Функція хешування “Купина” – національний стандарт України ДСТУ 7564:2014
60. Коди автентифікації повідомлень, що використовують функції хешування із ключем
61. CBC-MAC
62. Поняття про цифровий підпис (на прикладі RSA та Ель-Гамаля), вимоги до нього
63. Основні алгоритми електронного цифрового підпису, DSA
64. Стандарти ЕЦП Р 34.10 та Р 34.10-2001
65. Український алгоритм ЕЦП ДСТУ 4145
66. Стеганографічні системи. Модель та основні вимоги.
67. Відкриті, закриті та напівзакриті стеганосистеми.
68. Атаки на стеганографічні системи та протидія їм.
69. Пропускна здатність каналів приховуваної передачі повідомлень.
70. Оцінювання стійкості стеганографічних систем.
71. Методи стеганографії. Текстова стеганографія.
72. Методи стеганографії. Цифрова стеганографія.
73. Приховування даних у нерухомих цифрових зображеннях, відеофайлах та аудіо файлах.
74. Цифрові водяні знаки.
75. Методи модифікації найменшого значущого біта.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Технології захисту інформації/ Ю. А. Тарнавський. Київ: КПІ ім. Ігоря Сікорського, 2018. 162 с.
2. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.
3. Прикладна криптологія: системи шифрування: підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. К.: ДУТ, 2014. 448 с.
4. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.

Додаткова

5. Криптологія: навч. посібник/ М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. К.: Видавничий дім «Кондор», 2020. 248 с.
6. Основи криптології: навч. посібник/ Щур Н.О., Покотило О.А. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
7. Криптологія у прикладах, тестах і задачах: навч. посібник/ Т.В. Бабенко, Г.М. Гулак, С.О. Сушко, Л.Я. Фомичова. Д.: Національний гірничий університет, 2013. 318 с.
8. Історія криптології та секретного зв'язку/ Гребенніков В. В. Київ: Вид. «КНТ», 2023. 800 с.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/
2. Електронна бібліотека університету. URL: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php