ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

ЗАТВЕРДЖУЮ
Декан ФПКТКС
_____ Савенко О.С.
«___» _____ 2021 р.

СИЛАБУС
Навчальна дисципліна: "Прикладна криптологія"

Освітньо-професійна програма: «Кібербезпека»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Тітова Віра Юріївна
Профайл викладач(ів)	http://ksm.khnu.km.ua/sklad-kafedry/
E-mail викладача(ів)	v.titova231@gmail.com
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/course/view.php?id=6453
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/521227760 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2021-2022, семестр VI (зимово-весняний)
Розклад	
Консультації	

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
Д	3	6	7	210	85	34	34	17	-	125	-	-	-	+

Анотація дисципліни

Дисципліна формує у студентів знання про зміст і задачі криптографії та криптоаналізу; та навчає їх вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації; застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

Дисципліна викладається для студентів денної форми навчання спеціальності «Кібербезпека». При викладанні дисципліни використовуються наступні форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні, контекстні, тренінгові, застосування інформаційно-комп'ютерних технологій (CrypTool та інших).

Пререквізити: теорія передачі і захисту даних, технології безпечного програмування.

Кореквізити: проектно-технологічна практика, комплексні системи захисту інформації: проектування, впровадження, супровід.

Мета і завдання дисципліни

Метою викладання навчальної дисципліни «Прикладна криптологія» є формування компетентності майбутніх спеціалістів в галузі сучасних технологій криптографічного захисту інформації в комп'ютерних системах. Мета досягається через практичне оволодіння студентами навичками роботи з новітніми інформаційними технологіями у сфері криптографії та криптоаналізу, системами криптографічного захисту інформації; сучасним криптографічним програмно-апаратним забезпеченням інформаційно-комунікаційних технологій.

Предметом дисципліни є методи та стратегії, що реалізовані для управління процесу усунення несанкціонованого доступу з боку сторонніх користувачів; методики і напрями використання сучасних криптографічних алгоритмів; основи криптоаналізу; методи та засоби технічного та криптографічного захисту інформації.

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

компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях;

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

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

результати навчання:

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

РН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

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

РН 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* знання у практичних ситуаціях, у тому числі *адаптуватися* в умовах частої зміни технологій професійної

діяльності та *прогнозувати* кінцевий результат в задачах, пов'язаних з криптографічним захистом інформації; *застосовувати* криптографічні теорії та методи захисту, інформаційно-комунікаційні технології, сучасні методи і моделі інформаційної безпеки та/або кібербезпеки 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, *використовувати* компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності.

Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції**	Тема лаб. роботи ***	Тема практ. роботи ****	Самостійна роботи		
				Зміст	Год.	Література
1	**Введення в криптологію.** Основні поняття і визначення. Поняття криптографічної системи (КС)	-	**ПЗ1** Методи шифрування стовпцевої перестановки та подвійної перестановки	Опрацювання теоретичного матеріалу лекції №1. Виконання завдань ПЗ1.	7/8*	[1] с. 9-29, с. 145-148 [2] с.10-17, с. 26-29 [6] с. 14-40
2	**Структурна схема і математична модель криптографічних систем.** Структурна схема КС. Модель КС	**ЛР1** Криптографіч-ний захист інформації за допомогою шифрів стовпцевої перестановки та подвійної перестановки та оцінювання стійкості шифру	-	Опрацювання теоретичного матеріалу лекції №2. Підготовка до виконання ЛР1.	8/7*	[1] с. 20-29 [2] с.17-29 [3] с. 45-54 [7] с. 171-182 [10] с. 4-6
3	**Безумовно-стійкі криптографічні системи і їх реалізація.** Математична модель безумовно-стійких КС. Відстань рівнозначності у безумовно-стійких КС Умови реалізації безумовно-стійких КС	-	**ПЗ2** Метод шифрування простої заміни	Опрацювання теоретичного матеріалу лекції №3. Виконання завдань ПЗ2.	7/8*	[1] с. 29-38 [2] с.17-26, с. 29-31 [3] с. 45-54
4	**Умови реалізації обчислювально-стійких криптографічних систем.** Відстань рівнозначності для обчислювально-стійких КС. Умови реалізації обчислювально-стійких КС	**ЛР2** Криптографіч-ний захист інформації за допомогою шифрів простої заміни та оцінювання стійкості шифру	-	Опрацювання теоретичного матеріалу лекції №4. Підготовка до виконання ЛР2. Підготовка до захисту ЛР1.	8/7*	[1] с. 29-38 [2] с.17-26, с. 29-31 [3] с. 45-54 [10] с. 7-18

5	**Доказово-стійкі криптосистеми, їхня реалізація.** Класифікація і характеристика доказово-стійких КС. Афіні шифри. Потокові шифри. Блокові і складені шифри	-	**ПЗ3** Метод шифрування Цезаря	Опрацювання теоретичного матеріалу лекції №5. Виконання завдань ПЗ3.	7/8*	[1] с. 29-38, с. 61-68 [2] с.26-36 [6] с. 101-131
6	**Алгоритми і засоби формування ключів і паролів.** Вимоги до формування ключів і паролів. Лінійний рекурентний регістр. Лінійний конгруентний генератор	**ЛР3** Криптографіч-ний захист інформації за допомогою шифру Цезаря та оцінювання стійкості шифру	-	Опрацювання теоретичного матеріалу лекції №6. Підготовка до виконання ЛР3. Підготовка до захисту ЛР2.	8/7*	[1] с. 29-61 [2] с. 31-32 [10] с. 18-23
7	**Криптографічні системи з відкритими ключами і відкритим розподілом ключів**. RSA з відкритими ключами. Алгоритм крипто перетворення у КС з відкритими ключами. Генерація ключів Оцінка стійкості і складності ключів. Розподіл ключів по схемі Діффі-Гелмана	-	**ПЗ4** Метод шифрування Віжінера	Опрацювання теоретичного матеріалу лекції №7. Виконання завдань ПЗ4.	7/8*	[1] с. 61-66, с. 138-145 [2] с. 32-34, с. 36-47 [4] с. 189-213

8	**Крипто-перетворення в групах точок еліптичних кривих (ЕК).** Загальносистемні параметри перетворень на ЕК. Поняття еліптичної кривої над полем Галуа. Метрика операцій на ЕК. Методи побудови простих чисел і примітивних поліномів. Побудови і властивості базових точок на ЕК. Характеристика методів, визначення порядку в ЕК	**ЛР4** Криптографіч-ний захист інформації за допомогою шифру Віжінера та оцінювання стійкості шифру	-	Опрацювання теоретичного матеріалу лекції №8. Підготовка до захисту ЛР3. Підготовка до виконання ЛР4.	8/7*	[1] с. 61-66 [2] с. 32-34 [5] с. 109-115 [10] с. 23-38 [13] с. 65-102
9	**Методи побудови загальносистемних параметрів.** Метрика додавання і подвоєння в проективних координатах. Тест Рабінера-Міллера побудови простих чисел. Приклади розшифрування в розширених полях	-	**ПЗ5** Паролі та ключі, оцінювання стійкості	Опрацювання теоретичного матеріалу лекції №9. Виконання завдань ПЗ5.	7/8*	[2] с. 36-46 [12] с. 306-345
10	**Принципи реалізації спрямованого шифрування.** Спрямоване шифрування в кільцях і полях Методи спрямованого шифрування в групах точок ЕК	**ЛР5** Формування паролів та методи їх зламу за допомогою атак підбором	-	Опрацювання теоретичного матеріалу лекції №10. Підготовка до захисту ЛР4. Підготовка до виконання ЛР5.	8/7*	[5] с. 40-109 [11] с. 3-36
11	**Основні поняття і визначення теорії автентичності.** Основні поняття і визначення. Модель загроз в теорії автентичності. Вступ у теорію автентичності Сімонса	-	**ПЗ6** Алгоритм шифрування DES	Опрацювання теоретичного матеріалу лекції №11. Виконання завдань ПЗ6.	7/8*	[1] с. 71-79, с. 109-117 [2] с. 61-76 [8] с. 94-114

12	**Методи аутентифікації.** Основні положення теорії Класифікація методів аутентифікації	**ЛР6** Криптографічний захист інформації за допомогою алгоритмів шифрування DES та 3DES	-	Опрацювання теоретичного матеріалу лекції №12. Підготовка до захисту ЛР5. Підготовка до виконання ЛР6.	8/7*	[1] с. 71-79 [2] с. 61-76 [5] с. 272-284 [8] с. 94-114 [11] с. 45-56 [14] с. 60-77
13	**Методи забезпечення цілісності та достовірності у класі симетричних шифрів.** Методи аутентифікації в симетричних потокових системах. Методи аутентифікації в блокових симетричних системах	-	**ПЗ7** Алгоритм шифрування AES	Опрацювання теоретичного матеріалу лекції №13. Виконання завдань ПЗ7.	7/8*	[2] с. 76-91 [5] с. 284-325
14	**Поняття та властивості цифрового підпису (ЦП).** Поняття ЦП. Класифікація та вимоги до ЦП. Підписи в класі перетворень Ель-Гамаля та RSA. Поняття хеш-функції	**ЛР7** Криптографічний захист інформації за допомогою алгоритму шифрування AES	-	Опрацювання теоретичного матеріалу лекції №14. Підготовка до захисту ЛР6. Підготовка до виконання ЛР7.	8/7*	[2] с. 76-91 [9] с. 98-109 [11] с. 57-69 [14] с. 27-51
15	**Методи та алгоритми формування псевдовипадкових послідовностей.** Вимоги, пропоновані до псевдовипадкових послідовностей. Лінійна рекурентна послідовність з максимальним періодом. Псевдовипадкова послідовність на базі багатомодульних перетворень	-	**ПЗ8** Алгоритм шифрування RSA	Опрацювання теоретичного матеріалу лекції №15. Виконання завдань ПЗ8.	7/8*	[1] с. 79-88 [2] с. 102-117 [6] с. 135-172

16	**Випадкові послідовності.** Основні визначення випадкової послідовності Методи і засоби перевірки на випадковість	**ЛР8** Криптографіч-ний захист інформації за допомогою криптосистеми RSA і дослідження режимів її роботи	-	Опрацювання теоретичного матеріалу лекції №16. Підготовка до захисту ЛР7. Підготовка до виконання ЛР8.	8/8*	[1] с. 79-88 [2] с. 102-117 [6] с. 135-172 [11] с. 70-83
17	**Проблемні питання аутентифікації, як захисту інформації в інформаційно-телекомунікацій-них системах.** Теоретичні положення аутентифікації в інформаційно-телекомунікаційних системах Оцінювання автентичності в інформаційно-телекомунікаційних системах	Підсумкове заняття. **Контрольна робота**	-	Опрацювання теоретичного матеріалу лекції №17. Підготовка до захисту ЛР8. Підготовка до контрольної роботи.	4/5*	[5] с. 284-325 [15]

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)
** лекції проводяться по 2 години щотижня;
*** лабораторні проводяться по 4 години раз в два тижні.
**** практичні проводяться по 2 години раз в два тижні.

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/практичні заняття згідно з розкладом, не запізнюватися на заняття, вчасно виконувати та здавати лабораторні роботи та практичні завдання. 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. Термін здачі практики вважається своєчасним, якщо студент здав її в день виконання відповідної лабораторної роботи або до цього моменту. У випадку невиконання практики студент не допускається до виконання відповідної за темою та номером лабораторної роботи. Пропущене з поважної причини лабораторне заняття студент повинен відпрацювати у встановлений викладачем термін.

Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ https://www.khnu.km.ua/root/files/01/10/03/006.pdf.

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

	Аудиторна робота		**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Практичні заняття (мінімальна кількість оцінок - 8)	Лабораторні роботи	Контрольна робота	Семестровий контроль (іспит)
Тема	1		1-2	1-2
Ваговий коефіцієнт	0,15	0,25	0,2	0,4

Оцінювання практичних занять. Оцінка, яка виставляється за практичне заняття, складається з таких елементів: знання теоретичного матеріалу з теми; якість оформлення презентації виконаного завдання; вільне володіння студентом спеціальною термінологією і уміння застосовувати знання на практиці; своєчасна здача завдання з практики.

Оскільки виконане завдання з практики є допуском до виконання відповідної за темою та номером лабораторної роботи, то термін здачі практики вважається своєчасним, якщо студент здав її в день виконання відповідної лабораторної роботи або до цього моменту. У випадку невиконання практики студент не допускається до виконання відповідної за темою та номером лабораторної роботи та зобов'язаний здати виконане практичне завдання у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за практичне заняття викладач оголошує одразу після здачі і проставляє в електронний журнал дисципліни.

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 теоретичного питання та практичного завдання за темою одного з практичних занять. Оцінювання здійснюється за чотирибальною шкалою.

Оцінку «відмінно» отримує студент який дав повну письмову відповідь на теоретичне питання та правильно вирішив завдання, з обґрунтуванням вибору методів для його розв'язування.

Оцінку «добре» отримує студент, який дав правильну відповідь на теоретичне питання та правильно вирішив завдання, але у відповіді присутні дві-три несуттєві помилки, або є вагання з обґрунтуванням вибору методів вирішення.

Оцінку «задовільно» отримує студент, який дав часткову відповідь на теоретичне питання та допустив суттєві помилки при вирішення завдання.

Оцінку «незадовільно» отримує студент, який не зміг обрати правильні методи для вирішення завдання або не дав відповіді на теоретичне питання.

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 теоретичного питання 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. Задачі криптографії і криптоаналізу.
2. Задачі криптографічного захисту інформації
3. Блок-схема симетричної криптосистеми
4. Блок-схема асиметричної криптосистеми
5. Модульна арифметика.
6. Кінцеві структури: групи.
7. Зворотні елементи адитивної групи.
8. Зворотні елементи мультиплікативної групи.
9. Порядок групи і порядок елемента групи. Підгрупи.
10. Генератори групи і підгрупи.
11. Кількість генераторів груп і підгруп.
12. Циклічні і нециклічні групи
13. Кінцеві структури: кільця.
14. Мультиплікативна група кільця.
15. Кінцеві структури: поля.
16. Функція Ейлера.
17. Узагальнена функція Ейлера, що вона визначає.
18. Визначення НОД (a,b) за допомогою алгоритму Евкліда.
19. Мультиплікативна група кільця за модулем N = PQ.
20. Структура МГ кільця за модулем N = PQ.
21. Розподіл ключів по схемі Діффі-Гелмана (над кінцевим полем). Неінтерактивний протокол.
22. Розподіл ключів по схемі Діффі-Гелмана (над кінцевим полем). Інтерактивний протокол.
23. Криптосистема RSA. Функції шифрування-дешифрування.
24. Спрямоване шифрування RSA.
25. Цифровий підпис RSA.
26. Криптосистема Ель-Гамаля. Спрямоване шифрування.
27. Цифровий підпис Ель-Гамаля.
28. Цифровий підпис DSA
29. Основні поняття і визначення теорії автентичності.
30. Вступ у теорію автентичності професора Симонсона.
31. Методи аутентифікації. Основні положення теорії.
32. Класифікація методів аутентифікації
33. Методи забезпечення цілісності та достовірності у класі симетричних шифрів.
34. Методи аутентифікації в симетричних потокових системах.
35. Методи аутентифікації в блокових симетричних системах.
36. Методи та алгоритми формування псевдовипадкових послідовностей з m-ковою основою.
37. Вимоги, пропоновані до псевдовипадковим послідовностей.
38. Лінійна рекурентна послідовність з максимальним періодом.
39. Псевдовипадкова послідовність на базі багатомодульних перетворень.
40. Випадкові послідовності. Основні визначення випадкової послідовності.
41. Методи і засоби перевірки на випадковість.
42. Проблемні питання аутентифікації в каналах зв'язку.
43. Оцінка автентичності.
44. Особливості забезпечення послуг конфіденційності, цілісності, дійсності, приступності, спостерігаємості.
45. Афіні шифри. Потокові шифри. Блокові і складені шифри.
46. Алгоритми і засоби формування ключів і паролів. Вимоги.
47. Лінійний рекурентний регістр. Його властивості.
48. Лінійний конгруентний генератор.
49. Системи з відкритими ключами і відкритим розподілом ключів.
50. Генерація ключів. Оцінка стійкості і складності.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

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

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

№	Назва	Режим доступу
1.	Криптологія: навч.-метод. посіб. / Л.Я. Глинчук – Луцьк: Вежа-Друк, 2014. – 164 с.	http://www.dut.edu.ua/uploads/l_1887_91952284.pdf
2.	Технології захисту інформації / Ю. А. Тарнавський – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.	https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
3.	Кодирование и защита информации / П.Б. Акмаров. – Ижевск : ФГБОУ ВО Ижевская ГСХА, 2016. – 136 с.	https://www.docme.su/doc/1188620/5441.kodirovanie-i-zashhita-informacii.
4.	Основы криптографии/ Г.В. Басалова. – М.: ИНТУИТ, 2016. - 283 с.	https://www.twirpx.com/file/1907188/
5.	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.	https://drive.google.com/file/d/1Zqzz0pxqtm8KfmDnUvqYRWDYi0o6qsR_/view?usp=sharing
6.	Прикладна криптологія : системи шифрування: підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К.: ДУТ, 2014. – 448 с.	https://www.twirpx.com/file/2463828/
7.	Інформаційна та кібербезпека: соціотехнічний аспект. Підручник/ В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа. За заг. ред. докт. техн. наук, проф. В.Б. Толубко. – К.: ДУТ, 2015. – 288 с.	http://pdf.lib.vntu.edu.ua/books/2019/Buryachok_2018_320.pdf
8.	Конспект лекцій з дисципліни «Захист інформації у комп'ютерних системах» / Р.О. Жаровський. – Тернопіль, 2019. – 268 с.	http://elartu.tntu.edu.ua/bitstream/lib/29278/1/%21%21_Lek_print_zahust_123.pdf
9.	Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних. Посібник для викладачів, вчителів та студентів інформатичних спеціальностей./ В.М. Франчук – К.: НПУ імені М.П. Драгоманова, 2012. – 120 с.	https://vfranchuk.fi.npu.edu.ua/images/files/statty/32_ZIR_cript.pdf
10.	Методичні вказівки і завдання до лабораторних робіт з курсу «Комп'ютерна криптографія» [Електронний ресурс]/ укладач: О.М. Гапак. – Ужгород: УжНУ, 2015.	https://www.uzhnu.edu.ua/uk/infocentre/get/10972
11.	Методичні вказівки до виконання лабораторних робіт з дисципліни «Технології захисту інформації»/ А.О. Єгоров, Н.О. Соколова – Д.: НМетАУ, 2014. – 85 с.	http://repository.dnu.dp.ua:1100/upload/3d9cd5e2eeb927f627e43b0aa3f64314Technology-information-security.pdf
12.	Елементарна теорія чисел та елементи криптографії: підручник/ О. І. Клесов. - Київ : ТВіМС, 2016. – 412 с.	https://ela.kpi.ua/bitstream/123456789/30046/1/Elementarna_teoriia_chysel_ta_elementy_kryptohrafii.pdf
13.	Модели и методы синтеза сложных сигналов с необходимыми свойствами для защищенных телекоммуникационных систем. Диссертация на соискание ученой степени доктора технических наук / А.А. Замула. – Харьков, 2016. – 436 с.	http://kart.edu.ua/wp-content/uploads/2020/12/dus-zamula.pdf
14.	Криптографические методы защиты информации: учебное пособие [Електронний ресурс]./ Э.А. Болелов. – М.: МГТУ ГА, 2013.	http://89.218.140.251/ek/Болелов%20Э.А.%20Криптографические%20методы%20защиты%20информации.%20Часть%2

		02.%20Ассиметричные%20криптосистемы.pdf
15.	Аналіз існуючих підходів при ідентифікації і аутентифікації користувачів в інформаційно-телекомунікаційних системах/ О.С. Кульчицький, В.В. Грицюк, І.Г. Зотова. – Центр воєнно-стратегічних досліджень Національного університету оборони України ім. І. Черняховського, Київ. – 2016. – С. 60-64.	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjnwdGzv4ruAhXvs4sKHRWuBvUQFjAAegQIAxAC&url=http%3A%2F%2Fznp-cvsd.nuou.org.ua%2Farticle%2Fdownload%2F126048%2F120738&usg=AOvVaw2iVWZC3ty4EhrLJHu45rJ2

Додаткова

16.	Methods of cryptography. Study guide [Електронний ресурс]/ V. Stak. - Vilnius University, 2012.	http://www.mif.vu.lt/matinf/asm/vs/pask/crypto_prot/crpr_07/guide.pdf
17.	A Review of RSA Cryptosystems and Cryptographic Protocols/ P. O. Asagba, E. Nwachukwu// West African Journal of Industrial & Academic Research. - Vol.10 No.1. - 2014. – p. 3-16	https://www.ajol.info/index.php/wajiar/article/download/105736/95749
18.	Hybrid cryptographic technique using rsa algorithm and scheduling concepts/ M. Shankar, P. Akshaya// International Journal of Network Security & Its Applications (IJNSA)/ Vol.6, No.6. – 2014. - p. 39-48	https://pdfs.semanticscholar.org/0328/c75b2177fbfdf2433497ce6bbaccd061213f.pdf
19.	Sequence Alignment with Dynamic Divisor Generation for Keystroke Dynamics Based User Authentication/ Jiacang Ho, Dae-Ki Kang// Hindawi Publishing Corporation, Journal of Sensors. – 2015. – p. 1-14.	https://pdfs.semanticscholar.org/bafe/81b6b2f21e899cdc93d4cf401cf68c7d0dec.pdf
20.	Elliptic Curve Cryptology [Електронний ресурс]/ F. Rocco. – Union College - Schenectady, NY, 2017.	https://core.ac.uk/reader/229590739
21.	Cryptology and information security - past,present, and future role in society/ S. Bhattacharya. - International Journal on Cryptography and Information Security (IJCIS). – Vol. 9, No.1/2, 2019. – P. 13-36.	https://www.academia.edu/39778547/CRYPTOLOGY_AND_INFORMATION_SECURITY_PAST_PRESENT_AND_FUTURE_ROLE_IN_SOCIETY
22.	Криптоанализ шифрсистемы ACBF/ И. В. Боровкова, И. А. Панкратова. – Прикладная дискретная математика. Приложение, Томск. – 2019. – С. 90-93.	https://core.ac.uk/display/287384209?recSetID=
23.	Симетрична система з нелінійним шифруванням та можливістю контролю шифротексту з метою маскування/ В.М. Джулій, І.В. Муляр, В.С. Орленко, В.Ю. Тітова, В.А. Анікін// Вісник Хмельницького національного університету. Технічні науки. – 2020. – № 6. – С. 33-39.	http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/03/VKNU-TS-2020-N6-291.pdf
24.	Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. - Львів, «Магнолія 2006», 2016. – 256 с.	http://elartu.tntu.edu.ua/handle/123456789/18299
25.	Аналіз стеганографічних алгоритмів/ С. В. Лєнков, В. Ю. Тітова, І. В. Муляр, Р. М. Дацюк // Тези доповідей XVI Міжнародної науково-практичної конференції "Військова освіта і наука: сьогодення та майбутнє", 27 листоп. 2020 р. – Київ: ВІКНУ, 2020. – Т. 1. – С. 64–65.	http://elar.khnu.km.ua/jspui/handle/123456789/9656
26.	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.	http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/babenko_t_v_gulak_g_m_sushko_2013.pdf
27.	Аналіз поточного стану дій в області захищеної IP- телефонії / М. С. Гулечко, В. М. Джулій, В. Ю. Тітова // Збірник наукових праць молодих науковців і студентів «Інтелектуальний потенціал – 2020». – Хмельницький : ПВНЗ УЕП, 2020. – Ч. 2. – С. 35–39.	http://elar.khnu.km.ua/jspui/handle/123456789/9636

28.	The Evolution of Cryptology [Електронний ресурс]/ G. R. Souza. – California State University, San Bernardino, 2016.	https://core.ac.uk/reader/55336770
29.	Cryptology and communication security [Електронний ресурс]/ Shri Kant. – Defense Science Journal. – Vol. 62. - №1.	https://core.ac.uk/reader/333719963
30.	Криптологія в Інтернеті речей/ А.І. Петренко. – Київський національний економічний університет ім. В. Гетьмана, 2019. – С. 155-163.	https://kneu.edu.ua/userfiles/zb_mise/97/16.pdf

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань). Доступ до ресурсу: https://msn.khnu.km.ua.
2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Розробник _____ (Підпис) к.т.н., доцент (Вчений ступінь, звання) В.Ю. Тітова (Ініціали, прізвище)

Погоджено
Гарант освітньої програми _____ (Підпис) к.т.н., доцент (Вчений ступінь, звання) В.М. Чешун (Ініціали, прізвище)

Зав. кафедри кібербезпеки та комп'ютерних систем і мереж _____ (Підпис) к.т.н., доцент (Вчений ступінь, звання) Ю.П. Кльоц (Ініціали, прізвище)