ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету ІТ
Говорущенко Т.О.
«05» вересня 2024 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Криптологія
Назва

Статус дисципліни: вибіркова дисципліна
Факультет – Інформаційних технологій
Кафедра – Комп'ютерної інженерії та інформаційних систем

Фора здобуття освіти	Курс	Семестр	Загальне навантаження		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, в т.ч. ІРС			Залік	Іспит
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття						
ОД	1	парний	8	240	108	36	36	36		132			+	
Разом			**8**	**240**	**108**	**36**	**36**	**36**		**132**			**1**	

Програма складена _____ Капустян М.В.
Підпис Ініціали, прізвище викладача(ів)

Схвалена на засіданні кафедри Комп'ютерної інженерії та інформаційних систем

Протокол №2 від «30» серпня 2024 р.

Зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Засорнова І.О.
Підпис Ініціали, прізвище

Робоча програма розглянута та схвалена Вченою радою факультету інформаційних технологій

Протокол №1 від 05.09.2024 р.

Голова Вченої ради _____ Говорущенко Т.О.
Підпис Ініціали, прізвище

Хмельницький 2024

ВСТУП

Мета викладання дисципліни. Дисципліна "Криптологія" є однією з вибіркових дисциплін загальної підготовки у підготовці бакалаврів комп'ютерної інженерії.
Метою дисципліни "Криптологія" є освоєння студентами теоретичних і практичних основ криптології, криптографії та основ криптографічного аналізу, принципів розробки програмного забезпечення для їх реалізації на робочих станціях.

Предмет дисципліни. Сучасні стандарти інформаційної безпеки, інформаційні технології у галузі інформаційної безпеки, методи захисту інформації; розробка та впровадження технологій комп'ютерного захисту інформації, забезпечення цілісності даних, конфіденційності; контроль передачі інформації, ідентифікація, аутентифікація, криптографія, політика безпеки.

Завдання дисципліни. Надати студентам знання і практичні навички із використання криптології в комп'ютерних системах та мережах.

Після вивчення дисципліни "Криптологія" студент має досягти таких результатів навчання (сукупність знань, умінь, навичок, компетентностей):
знати:
- об'єкт, предмет, задачі, проблематику дисципліни та її основні розділи;
- наукові і математичні положення, що лежать в основі забезпечення криптографічного захисту; базові поняття й визначення, використовувані у галузі комп'ютерної інженерії;
- інновації у галузі криптографічного захисту інформації;

***уміти*:**
- застосовувати отримані знання для розв'язування задач налаштування та обслуговування технічних та програмних засобів захисту інформації відповідно до сучасних стандартів у галузі інформаційної безпеки;
- поєднувати теорію і практику криптографічного захисту, а також приймати оптимальні рішення при обслуговуванні та налаштуванні технічних та програмних засобів захисту;

бути здатним:
- розв'язувати складні задачі і проблеми в галузі криптографічного захисту інформації, що передбачає проведення досліджень та/або здійснення інновацій;
- діяти у складних і непередбачуваних умовах, що потребує застосування нових підходів, креативності, самостійного пошуку помилок, критичного оцінювання своєї поведінки та отриманих результатів;
- проводити дослідницьку та/або інноваційну діяльність в галузі інформаційної безпеки.

КРИПТОЛОГІЯ

Тип дисципліни	Вибіркова
Рівень вищої освіти	Перший (бакалаврський)
Мова викладання	Українська
Семестр	парний
Кількість встановлених кредитів ЄКТС	8,0
Форма здобуття освіти	Денна

Результати навчання
Студент, який успішно завершив вивчення дисципліни, повинен: вміло *використовувати* набуті знання з криптографії; *виконувати* основні задачі із забезпечення цілісності та конфіденційності інформації; *демонструвати* практичні навички із застосування криптографічних засобів захисту; *аналізувати* стан криптографічного захисту інформаційних ресурсів та ризики застосування криптографічного аналізу.

Зміст навчальної дисципліни.

Запланована навчальна діяльність: лекції – 36 год., практичні заняття – 36 год., лабораторні заняття – 36 год., самостійна робота – 132 год.; разом – 240 год.

Методи навчання: лекції (з використанням методів проблемного навчання і візуалізації); практичні заняття (з використанням практикумів); лабораторні заняття (з використанням тренінгів, майстер-класів), самостійна робота (індивідуальні завдання).

Форми оцінювання результатів навчання: захист лабораторних робіт.

Вид семестрового контролю: залік

Навчальні ресурси:

1. Криптологія. Навчальний посібник/ Лісовська Ю., Лісовський П., Курко П. –К: Кондор, 2020. -248 с.
2. Криптологія: навч.-метод. посіб. / Людмила Ярославівна Глинчук – Луцьк: Вежа-Друк, 2014. – 164 с.
3. Горбенко І. Д. // Прикладна криптологія: Теорія. Практика. Застосування / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Форт, 2013. – 880 с.
4. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Введ. 01–07–2015. – К. :Мінекономрозвитку України, 2015.
5. Задірака В.К. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: навч. посіб. / В. К. Задірака, А. М. Кудін, В. О. Людвиченко, О. С.Олексюк. – К. -Тернопіль: Підручники і посібники, 2007. – 272 с.
6. Захист інформації в комп'ютерних системах: підручник / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, О.О. Балюнов. –Ніжин: ФОП Лукяненко В.В., ТПК «Орхідея», 2020. -236 с.
7. Задірака В.К. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: навч. посіб. / В. К. Задірака, А. М. Кудін, В. О. Людвиченко, О. С.Олексюк. – К. -Тернопіль: Підручники і посібники, 2007. – 272 с.
8. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник / Г. Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с.
9. Корченко О. Г. Прикладна криптологія: системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.

Викладач: к.т.н., доцент Капустян М.В.

1. СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин, відведених на:			
	лекції	**практичні заняття**	**лабора-торні роботи**	**самостійну роботу**
Парний семестр				
1. Правила застосування шифру. Управління криптографією.	2	2	2	8
2. Політика інформаційної безпеки. Управління безпекою. Розробка правил безпеки. Вимоги до криптографічних систем.	2	2	2	12
3. Метод шифрування. Ключ шифрування.	4	4	4	16
4. Симетричні методи шифрування.	2	2	2	8
5. Несиметричні методи шифрування.	4	4	4	16
6. Проблеми та перспективи криптографічних систем.	2	2	2	8
7.Симетричне шифрування.	2	2	2	8
8. Асиметричне шифрування та його використання.	4	4	4	16
9. Управління ключами шифрування. Електронний цифровий підпис (ЕЦП). Особливості ЕЦП.	4	4	4	16
10. Поняття токенів. Еліптичне шифрування інформації.	2	2	2	8
11. Криптостійкість засобів ЕЦП.	2	2	2	8
12. Поняття електронного сертифікату. Моделі систем сертифікації. Проблеми та перспективи впровадження ЕЦП в Україні.	4	4	4	14
Разом за парний семестр:	**36**	**36**	**36**	**132**

Примітка. * по чисельнику – 18 годин, по знаменнику – 16 годин (розрахунок здійснюється відповідно до розкладу занять)

2. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1. Зміст лекційного курсу

Номер лекції	Перелік тем лекцій	Кількість годин
	Парний семестр	
1	Основні поняття криптології	2
2	Класичні шифри та їх крипоаналіз	2
3	Криптографічна стійкість шифрів	2
4	**Методи шифрування.** Симетричні методи шифрування. Асиметричні методи шифрування. Проблеми та перспективи криптографічних систем.	4
5	**Потокові симетричні шифри**	4
6	**Еліптичне шифрування інформації.** Поняття токенів. Еліптичне шифрування інформації.	2
7	**Електронний цифровий підпис (ЕЦП).** Призначення ЕЦП. Необхідність сертифікації засобів ЕЦП і відкритих ключів. Особливості рукописного підпису. Особливості ЕЦП.	2
8	**Криптостійкість засобів ЕЦП.** Поняття електронного сертифікату. Моделі систем сертифікації. Проблеми та перспективи впровадження ЕЦП в Україні.	4
9	Алгоритм блокового симетричного шифрування DES	2
10	Національний стандарт шифрування ДСТУ 7624:2014 («Калина»)	2
11	Режими шифрування блоків. Шифр IDEA	2
12	Елементи криптоаналізу шифрів. Нові напрямки в криптографії.	4
Разом за парний семестр:		**36**

2.2. Зміст лабораторних занять

№ п/п	Теми лабораторних робіт	К-ть годин
1	***Лабораторна робота №1.*** Криптографічні методи захисту інформації. Шифр Цезаря.	4
2	***Лабораторна робота №2.*** Шифрування методом поворотних решіток Кардано.	4
3	***Лабораторна робота №3.*** Симетричні методи шифрування.	4
4	***Лабораторна робота №4.*** Несиметричні методи шифрування.	4
5	***Лабораторна робота №5.*** Електронний цифровий підпис (ЕЦП).	6
6	***Лабораторна робота №6.*** Системи захисту в інформаційних мережах.	4
7	***Лабораторна робота №7.*** Електронний сертифікат. Адміністрування електронної пошти.	4
8	***Лабораторна робота №8.*** Програми виявлення вірусів та заходи по захисту та профілактиці.	6
Всього		**36**

2.3 Зміст самостійної (індивідуальної) роботи

Самостійна робота студентів денної форми навчання полягає у систематичному опрацюванні програмного матеріалу, підготовці до виконання і захисту лабораторних робіт, тестування з теоретичного матеріалу, виконанні індивідуальних завдань тощо.

Номер тижня	**Вид самостійної роботи**	К-ть годин
1.	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №1.	4
2.	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №1.	4
3.	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №1. Підготовка до лабораторної роботи №2.	12
4.	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №1. Підготовка до лабораторної роботи №3.	16
5.	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторних робіт №2. Підготовка до лабораторної роботи №3.	8
6.	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторних робіт №2,3. Підготовка до лабораторної роботи №4.	16
7.	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №3. Підготовка до лабораторної роботи №4.	8
8.	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №3,4. Підготовка до лабораторної роботи №5.	8
9.	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторних робіт №4. Підготовка до лабораторної роботи №5.	16
10.	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторних робіт №4,5. Підготовка до лабораторної роботи №6.	16
11.	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторних робіт №5. Підготовка до лабораторної роботи №6.	8
12.	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторних робіт №5,6. Підготовка до лабораторної роботи №7.	8
13.	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторних робіт №6. Підготовка до лабораторної роботи №7.	14
14.	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторних робіт №6,7. Підготовка до лабораторної роботи №8.	4
15.	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторних робіт №7. Підготовка до лабораторної роботи №8.	4

16.	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторних робіт №8. Підготовка до лабораторної роботи №8.	4
17.	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторних робіт.	2
	Разом за семестр:	**132**

3. МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться в основному словесними методами з використанням мультимедійних засобів. Лабораторні заняття проводяться у формі виконання реальних завдань і мають за мету набуття студентами практичних навичок із виявлення шкідливого програмного забезпечення, створення програмних продуктів із забезпечення інформаційної безпеки.

4. МЕТОДИ КОНТРОЛЮ ТА ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ У СЕМЕСТРІ

Поточний контроль здійснюється під час лекційних та лабораторних занять. Семестровий контроль проводиться у формі заліку. При цьому при виведенні остаточної оцінки враховуються результати поточного контролю.

Процес оцінювання підготовленості студента можна розділити на етапи:

Перший етап оцінювання спрямований на визначення знань інформаційного мінімуму. Якщо студент твердо засвоїв визначену навчальним планом суму формальних знань, то це означає, що він вміє використати їх при вирішенні різних питань при обслуговуванні комп'ютерів.

Перед вивченням дисципліни, як правило, проводиться вхідний контроль знань з дисциплін, що їй передують і забезпечують. При цьому необхідно встановити рівні та критерії сформованості знань щодо змісту навчальних елементів. Такими рівнями є:

Ознайомчо-орієнтовний (ОО) – особа має орієнтовне уявлення щодо понять, які вивчаються, здатна: відрізняти компоненти комп'ютера, периферійне та мережне обладнання.

Понятійно-аналітичний (ПА) – особа має чітке уявлення щодо навчального об'єкту, здатна перенести раніше засвоєні знання на типові ситуації.

Продуктивно-синтетичний (ПС) – особа має глибоке розуміння щодо навчального об'єкту, здатна здійснювати синтез, генерувати нові ідеї та уявлення, переносити раніше засвоєнні знання на нетипові, нестандартні ситуації.

Кожний вид роботи з дисципліни оцінюється за *чотирибальною* шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих *позитивно* з врахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих її видів робіт. Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (залік), вважається невстигаючим.

При оцінюванні знань студентів використовуються різні засоби контролю, зокрема: усне опитування перед допуском до виконання лабораторної роботи – здійснюється на її початку; засвоєння теоретичного матеріалу з тем перевіряється тестовим контролем; якість виконання, набуття теоретичних знань і практичних навичок перевіряється шляхом захисту кожної лабораторної роботи та індивідуального завдання згідно з робочою програмою дисципліни і робочим навчальним планом.

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 протоколу і графічної частини; вміння студента обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи. Для виконання програми дисципліни студент повинен отримати 8 оцінок за лабораторні роботи.

Термін захисту лабораторної роботи вважається своєчасним, якщо студент захистив її на наступному після виконання роботи занятті. За несвоєчасний захист лабораторної роботи з

неповажної причини студент за позитивну відповідь отримує оцінку «задовільно».

Пропущене лабораторне заняття студент повинен 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.

При *оцінюванні знань* студентів викладач керується такими критеріями.

Оцінку «відмінно» отримує студент за глибоке і повне опанування змісту навчального матеріалу, в якому він легко орієнтується, понятійного апарату, за уміння зв'язувати теорію з практикою, вирішувати практичні завдання, висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає грамотний, логічний виклад відповіді (як в усній, так і в письмовій формі), якісне зовнішнє оформлення. Студент повинен набути практичних навичок із обслуговування комп'ютерів, периферійного та мережного обладнання.

Оцінка «відмінно» виставляється студенту, який вміє раціонально застосувати основні принципи і методи обслуговування комп'ютерів та вміє ними користуватися. Студент не повинен вагатися при видозміні запитання, повинен робити детальні та узагальнюючі висновки.

Оцінку «добре» отримує студент за повне засвоєння навчального матеріалу, володіння понятійним апаратом, орієнтування у вивченому матеріалі, свідоме використання знань для вирішення практичних завдань, грамотний виклад відповіді, але у змісті і формі відповіді мали місце окремі неточності (похибки), нечіткі формулювання закономірностей тощо. Відповідь студента повинна будуватись на основі самостійного мислення.

Оцінку «добре» отримує студент за правильну відповідь з однією-двома суттєвими помилками.

Оцінки «задовільно» заслуговує студент, який виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, що справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент слабо знає структуру курсу, допускає помилки у відповіді, засвоїв і набув практичних навичок у обслуговування комп'ютерів, складанні та розбиранні їх, орієнтується в призначенні компонентів комп'ютера, але допустив неточності. Вагається при відповіді на видозмінене запитання, разом з тим студент володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.

Оцінки «задовільно» заслуговує студент за неповне опанування програмного матеріалу, але отримані знання і набуті практичні навички з основ інформаційних технологій.

Оцінка «незадовільно» виставляється, коли студент має розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, припускається 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 додаткових знань з курсу.

На основі результатів поточного контролю і підсумкового контрольного заходу виставляється підсумкова семестрова оцінка. На основі аналізу контролю знань викладач удосконалює курс лекцій, звертаючи особливу увагу на ті розділи, чи теми, з яких було найбільше неточних відповідей, що свідчить про методичні чи інші недоліки при висвітленні вказаних тем або розділів.

Аналогічно вносяться корективи в методичні посібники для лабораторних робіт, детальніше розглядаються принципові питання при виконанні лабораторних робіт та їх захисту.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів денної форми навчання у семестрі за ваговими коефіцієнтами

Аудиторна робота								Семестр. контроль (залік)
парний семестр								
Лабораторні роботи №:								Залік за рейтингом
1	2	3	4	5	6	7	8	
ВК: 1								

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

Якщо студент отримав негативну оцінку, 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".

Підсумкова семестрова оцінка за національною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення усіх оцінок до електронного журналу. Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС наведені у наступній таблиці.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	Інтервальна шкала балів	Вітчизняна оцінка	
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

5. ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ СТУДЕНТІВ

1. Загальні поняття захисту інформації.
2. Закони України про захист інформації.
3. Аналіз даних захисту.
4. Право інтелектуальної власності та політика інформаційної безпеки.
5. Управління безпекою.
6. Розробка правил безпеки.
7. Міжнародні правила застосування шифру.
8. Управління криптографією.
9. Вимоги до криптографічних систем.
10. Метод шифрування.
11. Ключ шифрування.
12. Симетричні методи шифрування.
13. Несиметричні методи шифрування.
14. Проблеми та перспективи криптографічних систем.
15. Симетричне шифрування.
16. Асиметричне шифрування та його використання.

17. Управління ключами шифрування.
18. Правовий статус електронного цифрового підпису
19. Призначення електронного підпису.
20. Необхідність сертифікації засобів ЕЦП і відкритих ключів.
21. Особливості рукописного підпису.
22. Особливості ЕЦП.
23. Поняття токенів.
24. Еліптичне шифрування інформації.
25. Загальна характеристика систем захисту в інформаційних мережах.
26. Фізична безпека.
27. Аутентифікація та безпека мережі.
28. Паролі.
29. Захист інформації в бездротових локальних мережах.
30. Криптостійкість засобів ЕЦП.
31. Поняття електронного сертифікату.
32. Моделі систем сертифікації.
33. Проблеми та перспективи впровадження ЕЦП в Україні.
34. Правове регулювання ЕЦП в Україні та світі.
35. Алгоритм цифрового підпису Шнорра.
36. Сліпий підпис, незаперечний підпис, груповий підпис.
37. Криптографічні протоколи
38. Вимоги до протоколів автентифікації.
39. Модель загроз порушення автентичності.
40. Модель взаємної недовіри та взаємного захисту.
41. Основи криптографії на еліптичних кривих
42. Алгоритм обчислення порядку еліптичної кривої.
43. Криптосистема Мессі-Омури над групою точок еліптичної кривої.
44. Аналіз вразливостей криптографічної схеми цифрового підпису ECDSA.
45. Елементи криптоаналізу шифрів
46. Силові методи криптоаналізу.
47. Криптоаналіз по побічним каналам.
48. Нові напрямки в криптографії
49. Стеганографія та її застосування.

6. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни «Криптологія» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою.

7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Криптологія. Навчальний посібник/ Лісовська Ю., Лісовський П., Курко П. –К: Кондор, 2020. -248 с.
2. Криптологія: навч.-метод. посіб. / Людмила Ярославівна Глинчук – Луцьк: Вежа-Друк, 2014. – 164 с.
3. Горбенко І. Д. // Прикладна криптологія: Теорія. Практика. Застосування / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Форт, 2018. – 880 с.
4. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Введ. 01–07–2015. – К. :Мінекономрозвитку України, 2015.
5. Захист інформації в комп’ютерних системах: підручник / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, О.О. Балюнов. –Ніжин: ФОП Лукяненко В.В., ТПК «Орхідея», 2020. -236 с.
6. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник / Г. Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с.

8. ІНФОРМАЦІЙНІ РЕСУРСИ

Електронний університет:

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі тестові завдання для поточного та семестрового контролю знань).
2. Електронна бібліотека університету