Силабус навчальної дисципліни
"Прикладна криптологія"

Спеціальність: 125, Кібербезпека
Галузь знань: 12, Інформаційні технології

Рівень вищої освіти	Перший (бакалаврський)
Статус дисципліни	Навчальна дисципліна обов'язкового компонента циклу професійної підготовки
Курс	III (третій), IV (четвертий)
Семестр	V (п'ятий), VI (шостий), VII (сьомий)
Обсяг дисципліни, кредити ЄКТС/загальна кількість годин	9,5 кредитів / 285 годин
Мова викладання	Українська
Що буде вивчатися (предмет навчання)	Методи, алгоритми, протоколи та системи криптографічного захисту інформації
Чому це цікаво/потрібно вивчати (мета)	Отримання курсантами методологічних основ побудови та аналізу алгоритмів та систем криптографічного захисту інформації.
Чому можна навчитися (результати навчання)	РН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційнотелекомунікаційних системах. РН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. РН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки. РН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. РНвс 2. Проектувати та впроваджувати системи (елементи) криптографічного захисту інформації в Збройних Силах України та Міністерства оборони України. РНвс 15. Вдосконалення методики, способів та прийомів застосування систем (елементів) захисту інформації та кібербезпеки в інформаційно-телекомунікаційних системах Збройних Сил України та Міністерства оборони України.

Як можна користуватися набутими знаннями і уміннями (компетентності)	ФК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики та стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. ВСК 1. Здатність створювати, впроваджувати та розгортати системи (елементи) захисту інформації (технічного, криптографічного, організаційного) та кібербезпеки в Збройних Силах України та Міністерства оборони України.
Навчальна логістика	**Зміст навчальної дисципліни:** **Змістовний модуль 1.** Основи теорії чисел Заняття 1/1. Арифметика цілих чисел. Заняття 1/2. Лінійні діофантові рівняння Заняття 1/3. Рішення математичних задач з використанням теорії подільності. Заняття 1/4. Арифметика залишків. Заняття 1/5. Дослідження властивостей операцій за модулем. Заняття 1/6. Лінійне порівняння. Заняття 1/7. КТЗ. Заняття 1/8. Рішення задач з КТЗ. Заняття 1/9. Прості числа. Заняття 1/10. Використання теореми Ейлера для вирішення прикладних задач. Заняття 1/11. Тестування простих чисел. Заняття 1/12. Практична реалізація тестування простих чисел. **Змістовий модуль 2**. Основи прикладної алгебри Заняття 2/1. Групи та властивості груп. Заняття 2/2. Побудова групових операцій. Порядок групи та порядок елемента групи Заняття 2/3. Поняття кільця та поліному над кільцем. Заняття 2/4. Поле та побудова полів. Заняття 2/5. Реалізація операцій в полях. Заняття 2/6. Еліптичні криві над полями. Заняття 2/7. Реалізація операцій в полях. Заняття 2/8. Еліптичні криві над розширеннями поля характеристики 2. Заняття 2/9. Рішення задач щодо оцінки стійкості операцій скалярного множення точок еліптичної кривої.

Змістовий модуль 3. Принципи побудови та аналізу симетричних криптографічних систем

Заняття 3/1. Вступ
Заняття 3/2. Загальні поняття про симетричні криптосистеми та їх криптоаналіз.
Заняття 3/3. Принципи побудови моноалфавітних шифрів.
Заняття 3/4. Криптоаналіз адитивних, мультиплікативних та афінних шифрів.
Заняття 3/5. Програмна реалізація криптоалгоритмів моноалфавітних шифрів.
Заняття 3/6. Принципи побудови багатоалфавітних шифрів підстановки.
Заняття 3/7. Шифр Віженера та його криптоаналіз.
Заняття 3/8. Дослідження багатоалфавітних шифрів.
Заняття 3/9. Принципи побудови шифрів перестановки.
Заняття 3/10. Криптоаналіз шифрів перестановки. Шифри з подвійною перестановкою.
Заняття 3/11. Шифри потоку та блокові шифри.
Заняття 3/12. Основи сучасних блокових шифрів з симетричним ключем.
Заняття 3/13. Компоненти сучасного блокового шифру.
Заняття 3/14. Дослідження структури складових шифрів.
Заняття 3/15. Криптоаналіз сучасних блокових шифрів.
Заняття 3/16. Сучасні шифри потоку.
Заняття 3/17. Стандарт шифрування даних DES.
Заняття 3/18. Стандарт шифрування даних DES.
Заняття 3/19. Дослідження криптостійкості DES.
Заняття 3/20. Дослідження багатократного використання DES.
Заняття 3/21. Удосконалений стандарт шифрування AES.
Заняття 3/22. Дослідження криптографічних перетворень AES.
Заняття 3/23. Розширення ключів в AES.
Заняття 3/24. Приклади розширення ключів в AES.
Заняття 3/25. Дослідження проектів реалізації AES та його аналіз.
Заняття 3/26. Стандарт шифрування даних ДСТУ ГОСТ 28147:2009.
Заняття 3/27. Дослідження режимів роботи ДСТУ ГОСТ 28147:2009.
Заняття 3/28. Стандарт шифрування даних ДСТУ 7624:2014.
Заняття 3/29. Дослідження режимів роботи ДСТУ ГОСТ 28147:2009.
Заняття 3/30. Стандарт шифрування даних ДСТУ 7624:2014.
Заняття 3/31. Режими роботи сучаснихблокових шифрів.
Заняття 3/32. Потокові системи шифрування.
Заняття 3/33. Дослідження режимів роботи потокових системи шифрування.
Заняття 3/34. Оцінка стійкості потокових системи шифрування.

Змістовий модуль 4. Асиметричні криптосистеми. Геш-функції

Заняття 4/1. Вступ
Заняття 4/2. Цілісність повідомлень.
Заняття 4/3. Встановлення дійсності повідомлення.
Заняття 4/4. Ітеративні ґеш-функції.
Заняття 4/5. Дослідження алгоритму безпечного ґешування SHA-512.
Заняття 4/6. Дослідження ітеративної функції криптографічного ґешування Whirlpool.
Заняття 4/7. Стандарти функції ґешування.
Заняття 4/8. Загальні поняття асиметрично-ключових криптосистем.
Заняття 4/9. Ранцева криптосистема.
Заняття 4/10. Криптографічна система RSA.
Заняття 4/11. Загальні положення про цифровий підпис.
Заняття 4/12. Схема цифрового підпису RSA.
Заняття 4/13. Дослідження схем цифрових підписів.

	Заняття 4/14. Дослідження схеми цифрового підпису на еліптичних кривих. Заняття 4/15. Стандарти цифрового підпису.

	Змістовий модуль 5. Асиметричні протоколи Заняття 5/1. Автентифікація об’єкту. Заняття 5/2. Автентифікація суб’єкту. Заняття 5/3. Автентифікація за допомогою функції ”запит-відповідь“. Заняття 5/4. Автентифікація асиметричними методами. Заняття 5/5. Дослідження протоколів з нульовим розголошенням. Заняття 5/6. Управління ключами з використанням симетричного шифрування. Заняття 5/7. Протокол встановлення достовірності Kerberos. Заняття 5/8. Дослідження методів погодження симетричних ключів. Заняття 5/9. Управління ключами з використанням асиметричного шифрування. Заняття 5/10. Управління ключами з використанням асиметричного шифрування. Заняття 5/11. Інфраструктура відкритих ключів. Заняття 5/12. Налаштування інфраструктури відкритих ключів. Заняття 5/13. Налаштування інфраструктури відкритих ключів II. Заняття 5/14. Налаштування інфраструктури відкритих ключів I. **Види занять**: лекції, групові, практичні **Методи навчання:** пояснювально-ілюстраційний, репродуктивний, онлайн **Форми навчання**: очна, заочна
Пререквізити	Вища математика; Теорія ймовірностей, імовірнісні процеси та математична статистика
Пореквізити	Криптографічний захист в спеціальних інформаційних системах, Засоби криптографічного захисту інформації в спеціальних ІТС, Засоби захисту інформації в кіберпросторі

Інформаційне забезпечення з фонду та репозитарію ВІТІ	**Науково-технічна бібліотека ВІТІ:** 1. Ємець В., Мельник А., Попович Р. Сучасна криптографія. Основні поняття. – Львів: Бак, 2003. – 144 с. 2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Монографія. – Харків: видавництво «Форт», 2012. – 880 с.
Локація та матеріально-технічне забезпечення	Аудиторія теоретичного навчання, мультимедійний проектор, ПЕОМ
Семестровий контроль, екзаменаційна методика	диференційований залік, іспит, іспит
Кафедра	Кібербезпеки
Факультет	Бойового застосування систем управління та зв'язку
Викладач(і)	 **Чевардін Владислав Євгенійович** **Посада: Начальник кафедри** **Вчене звання: Старший науковий співробітник** **Науковий ступінь: Доктор технічних наук** **Профайл викладача:** **Тел.:** *443-22* **E-mail:** vladyslav.chevardin@gmail.com **Робоче місце**: *436** **Самойлов Ігор Володимирович** **Посада: Доцент кафедри** **Вчене звання: Доцент** **Науковий ступінь: Кандидат технічних наук** **Профайл викладача:** **Тел.:** *443-22* **E-mail:** samoilov1966igor@gmail.com **Робоче місце**: *442** **Яковлєв Сергій Володимирович** **Посада: Доцент кафедри** **Вчене звання:** **Науковий ступінь: Кандидат технічних наук** **Профайл викладача:** **Тел.:** *443-22* **E-mail:** yasv@rl.kiev.ua **Робоче місце**: *442**
Оригінальність навчальної дисципліни	
Лінк на дисципліну	http://212.111.203.250:4213/moodle/course/view.php?id=351#section-4

СТРУКТУРА КРЕДИТНОГО МОДУЛЯ

№№ з/п	Види НЗ	Кількість годин	Із них		Номери семестрів, назва змістового модуля, тем занять, навчальні питання	Матеріально-технічне забезпечення	Інформаційно-методичне забезпечення
			Аудиторних годин	Самостійна робота			
Семестр 5							
Змістовий модуль 1. <u>Основи теорії чисел</u>							
1.	Лекція № 1	3	2	1	**<u>Заняття 1/1. Арифметика цілих чисел.</u>** 1. Теорія подільності цілих чисел. 2. Основна теорема арифметики. 3. Алгоритм Евкліда. 4. Бінарні операції над цілими числами. **Самостійна робота 2** Програмна реалізація алгоритму Евкліда.	дошка, крейда демонстр. матеріал	[2] с. 37-43, [9, 10].
2.	Лекція № 2	3	2	1	**<u>Заняття 1/2. Лінійні діофантові рівняння.</u>** 1.Деякі положення теорії подільності. 2.Мала Теорема Ферма. Теорема Ойлера. 3.Лінійні діофантові рівняння. Загальне та приватні рішення. **Самостійна робота 3** Програмна реалізація розширеного алгоритму Евкліда.		
3.	Групове заняття № 1	3	2	1	**<u>Заняття 1/3. Рішення математичних задач з використанням теорії подільності.</u>** 1.Відношення порівняння. Розв'язання рівнянь на основі модульної арифметики. 2.Система залишків. Бінарні операції в системі залишків. **Самостійна робота 3** Програмна реалізація рішення лінійного діофантового рівняння.	дошка, крейда демонстр. матеріал	[2] с. 43-47, [9, 10].
4.	Групове заняття № 2	3	2	1	**<u>Заняття 1/4. Арифметика залишків.</u>** 1. Адитивна інверсія, 2. Мультиплікативна інверсія. 3. Використання розширеного алгоритму Евкліда. 4. Таблиці додавання та множення. **Самостійна робота 4** Програмна реалізація бінарних операції в системі залишків.	дошка, крейда демонстр. матеріал	[2] с. 47-54, [9, 10].
5.	Практичне заняття № 1	6	4	2	**<u>Заняття 1/5. Дослідження властивостей операцій за модулем.</u>** 1. Рішення практичних задач з модульної арифметики. 2.Програмна реалізація модульних операцій. 3.Програмна реалізація мультиплікативної інверсії.	комп'ютерний клас, середовище C++, C#	[2] с. 54-59, [9, 10].

					4. Програмна реалізація розширеного алгоритму Евкліда для пошуку мультиплікативної інверсії. **Самостійна робота 5** Створення бібліотеки програмних математичних функцій.		
6.	Групове заняття № 3	3	2	1	**<u>Заняття 1/6. Лінійне порівняння.</u>** 1. Лінійне рівняння з одним невідомим. 2. Схема Горнера. 3. Рішення практичних задач. **Самостійна робота 6** Програмна реалізація операцій над матрицями.	дошка, крейда демонстр. матеріал	[2] с. 59-64, [9, 10].
7.	Групове заняття № 4	3	2	1	**<u>Заняття 1/7. КТЗ</u>**. 1. КТЗ 2.Факторизація чисел. 3. Рішення практичних задач. **Самостійна робота 7** Програмна реалізація алгоритмів розв'язання систем лінійних рівнянь.	дошка, крейда демонстр. матеріал	[2] с. 64-66, [9, 10].
8.	Практичне заняття №2	4	2	2	**<u>Заняття 1/8. Рішення задач з КТЗ.</u>** 1. Рішення задач з функцією Ойлера. 2. Рішення задач з МТФ, з Т Ойлера. 3. Програмна реалізація функції Ойлера. **Самостійна робота 8** Програмна реалізація обчислення детермінанту та мультиплікативної інверсії	дошка, крейда демонстр. матеріал	[2] с. 59-72, [9, 10].
9.	Лекція № 3	3	2	1	**<u>Заняття 1/9. Прості числа.</u>** 1. Символ Лежандра. 2. Символ Якоби. 3. Квадратні корені за модулем. **Самостійна робота 9** Вивчення алгоритмів пошуку простих чисел (імовірнісних та детермінованих).	дошка, крейда демонстр. матеріал	[2] с. 276-281, [9, 10].
10.	Практичне заняття № 3	4	2	2	**<u>Заняття 1/10. Використання теореми Ейлера для вирішення прикладних задач.</u>** 1.Рішення задач на символ Лежандра. 2. Рішення задач на символ Якоби. 3. Рішення задач на квадратні корені за модулем. **Самостійна робота 10** Програмна реалізація генераторів простих чисел.	дошка, крейда демонстр. матеріал	[2] с. 281-284, [9, 10].
11.	Лекція № 4	3	2	1	**<u>Заняття 1/11. Тестування простих чисел.</u>** 1. Детерміновані алгоритми. 2. Імовірнісні алгоритми. 3. Рекомендовані тести простих чисел. **Самостійна робота 11** Програмна реалізація детермінованих алгоритмів	дошка, крейда демонстр. матеріал	[2] с. 284-291, [9, 10].
12.	Практичне заняття № 4	4	2	2	**<u>Заняття 1/12. Практична реалізація тестування простих чисел.</u>** 1. Детерміновані алгоритми. 2. Імовірнісні алгоритми. **Самостійна робота 12**	дошка, крейда демонстр.	[2] с. 292-301, [9, 10].

					Наслідки китайської теореми про залишки.	матеріал	

Змістовий модуль 2 Основи прикладної алгебри							
13.	Лекція № 5	3	2	1	**Заняття 2/1. Групи та властивості груп.** 1.Поняття групи, абелевої групи. 2.Циклічні групи. 3. Підгрупи. 4. Підгрупи породжені елементом. **Самостійна робота 13** Квадратичне порівняння за модулем, що складається.	дошка, крейда демонстр. матеріал	[2] с. 301-304, [9, 10].
14.	Групове заняття № 5	3	2	1	**Заняття 2/2. Побудова групових операцій. Порядок групи та порядок елемента групи** 1. Приклади побудови груп на числах та лишках, таблиці Келі. 2. Порядок групи, порядок елементу групи. 3. Теорема Лагранжа та її застосування. **Самостійна робота 14** Програмна реалізація алгоритму зведення до ступеня.	дошка, крейда демонстр. матеріал	[2] с. 304-306, [9, 10].
15.	Групове заняття № 6	4	2	2	**Заняття 2/3. Поняття кільця та поліному над кільцем.** 1.Поняття кільця, властивості кільця. 2. Поняття поліному над кільцем 3. Алгоритм Евкліда для поліномів. **Самостійна робота 14** Програмна реалізація алгоритму зведення до ступеня.	метод. матеріал	[2, 9, 10].
16.	Лекція № 6	3	2	1	**Заняття 2/4. Полє та побудова полів**. 1. Поняття поля 2. Властивості полів. 3. Подання поля, генератор поля, поліноміальний базис. **Самостійна робота 15** Побудова власної групи, кільця та поля.	дошка, крейда демонстр. матеріал	[2] с. 119-121, 126-128, [9, 10].
17.	Групове заняття № 7	3	2	1	**Заняття 2/5. Реалізація операцій в полях.** 1. Додавання, множення, піднесення до степеню у полі. 2. Інверсія в полі. **Самостійна робота 16** Програмна реалізація операцій в полях Галуа.	дошка, крейда демонстр. матеріал	[2] с. 122-126, 128-130 [9, 10].
18.	Лекція № 7	3	2	1	**Заняття 2/6. Еліптичні криві над полями.** 1. Нормальна та канонічна форма кривої. 2. Група точок кривої. 3. Скалярне множення точок еліптичної кривої. **Самостійна робота 17** Програмна реалізація операцій с поліном-модулем.	дошка, крейда демонстр. матеріал	[2] с. 130-132, [9, 10].

19.	Практичне заняття № 5	4	4	6	**Заняття 2/7. Реалізація операцій в полях.** 1.Побудова еліптичної кривої. 2. Реалізація операцій над групою точок кривої. **Самостійна робота 18** Використання генератора для визначення полів $GF(2^n)$.	дошка, крейда демонстр. матеріал	[2] с. 132-139, [9, 10].
20.	Лекція № 8	2	2		**Заняття 2/8. Еліптичні криві над розширеннями поля характеристики 2.** 1. Нормальна та канонічна форма кривої. 2. Група точок кривої. 3. Скалярне множення точок еліптичної кривої.		
21.	Практичне заняття № 9	4	2	2	**Заняття 2/9. Рішення задач щодо оцінки стійкості операцій скалярного множення точок еліптичної кривої.** 1. Додавання, інверсія точок кривої. 2. Скалярне множення точок кривої. 3. Обчислення порядку точок кривої.		
22.	Групове заняття № 8	2	2		**Модульна контрольна робота**		
23.	Групове заняття №9	2	2		**Залік**		
Разом		**81**	**50**	**31**			

Семестр 6							
Змістовий модуль 3. Принципи побудови та аналізу симетричних криптографічних систем							
1.	Лекція № 1	3	2	1	**Заняття 3/1. Вступ** 1. Цілі підтримки інформаційної безпеки. 2. Послуги та механізми інформаційної безпеки. 3. Методи реалізації механізмів інформаційної безпеки. **Самостійна робота 1** Методи реалізації механізмів інформаційної безпеки.	дошка, крейда, демонстр. матеріал	[1] с. 86-95, [2] с. 15-33.
2.	Лекція № 2	3	2	1	**Заняття 3/2. Загальні поняття про симетричні криптосистеми та їх криптоаналіз.** 1. Загальна ідея шифрування симетрич-ним ключем. 2. Типи атак криптоаналізу. **Самостійна робота 2** Типи атак криптоаналізу.	дошка, крейда демонстр. матеріал	[2] с. 73-79.
3.	Лекція № 3	3	2	1	**Заняття 3/3. Принципи побудови моноалфавітних шифрів.** 1. Адитивний шифр. 2. Мультиплікативний шифр. 3. Афінний шифр. 4. Моноалфавітний шифр підстановки. **Самостійна робота 3** Моноалфавітний шифр підстановки	дошка, крейда демонстр. матеріал	[1] с. 99-122, [2] с. 79-88.

4.	Практичне заняття № 1	3	2	1	**Заняття 3/4. Криптоаналіз адитивних, мультиплікативних та афінних шифрів.** 1. Атака грубої сили. 2. Статистична атака. 3. Атака з вибором вихідного тексту. **Самостійна робота 4** Атака з вибором вихідного тексту.	дошка, крейда демонстр. матеріал	[1] с. 99-122, [2] с. 79-88.
5.	Практичне заняття № 2	3	2	1	**Заняття 3/5. Програмна реалізація криптоалгоритмів моно-алфавітних шифрів.** 1. Програма шифрування (розшифру-вання) адитивного шифру. 2. Програма шифрування (розшифрування) мультиплікативного шифру. 3. Програма шифрування (розшифрування) афінного шифру. 4. Програма реалізація статистичної атаки. **Самостійна робота 5** Програма реалізація статистичної атаки.	дошка, крейда демонстр. матеріал	[1] с. 99-122, [2] с. 73-88.
6.	Лекція № 4	3	2	1	**Заняття 3/6. Принципи побудови багатоалфавітних шифрів підстанов-ки.** 1. Автоключовий шифр та його криптоаналіз. 2. Шифр плейфеера та його криптоаналіз. **Самостійна робота 6** Поліалфавитні шири та їх криптоаналіз.	дошка, крейда демонстр. матеріал	[1] с. 101-122, [2] с. 89-92.
7.	Групове заняття № 1	2	2	1	**Заняття 3/7. Шифр Віженера та його криптоаналіз.** 1. Загальні положення. 2. Порядок шифрування та розшифру-вання. 3. Криптоаналіз шифру Віженера.	дошка, крейда демонстр. матеріал	[1] с. 101-122, [2] с. 92-95.
8.	Практичне заняття № 3	3	2	1	**Заняття 3/8. Дослідження багато-алфавітних шифрів**. 1. Одноразовий блокнот. 2. Роторний шифр. 3. Машина “Енігма”. **Самостійна робота 7** Машина “Енігма”.	дошка, крейда демонстр. матеріал	[2] с. 98-102.
9.	Групове заняття № 2	2	2	1	**Заняття 3/9. Принципи побудови шифрів перестановки.** 1. Безключові шифри перестановки. 2. Ключові шифри перестановки. 3. Комбіновані шифри перестановки. 4. Ключі шифрування та розшифрування. 5. Приклад використання матриць для шифрування.	дошка, крейда демонстр. матеріал	[2] с. 102-106.
10.	Практичне заняття № 4	2	2		**Заняття 3/10. Криптоаналіз шифрів перестановки. Шифри з подвійною перестановкою.** 1. Методи криптоаналізу шифрів перес-тановки. 2. Шифри з подвійною перестановкою.	дошка, крейда демонстр. матеріал	[2] с. 106-109.

11.	Лекція № 5	3	2	1	**Заняття 3/11. Потокові та блокові шифри.** 1. Потокові шифри. 2. Блокові шифри. 3. Шифри гамування. 4. Загальна класифікація шифрів. **Самостійна робота 8** Блокові шифри.	дошка, крейда демонстр. матеріал	[2] с. 109-111.
12.	Лекція № 6	3	2	1	**Заняття 3/12. Основи сучасних блокових шифрів з симетричним ключем.** 1. Сучасні блокові шифри. 2. Повнорозмірні ключові шифри. 3. Шифри ключа часткового розміру. 4. Шифри без ключа. **Самостійна робота 8** Шифри без ключа.	дошка, крейда демонстр. матеріал	[2] с. 144-150.
13.	Групове заняття № 3	2	2		**Заняття 3/13. Компоненти сучасного блокового шифру.** 1. P-блоки. 2. S-блоки.	дошка, демонстр. матеріал	[2] с. 150-154.
14.	Практичне заняття №5	3	2	1	**Заняття 3/14. Дослідження структури складових шифрів.** 1. Шифри Файстеля. 2. Шифри не-Файстеля. **Самостійна робота 9** Шифри не-Файстеля.	дошка, крейда демонстр. матеріал	[2] с. 162-166.
15.	Групове заняття № 4	2	2		**Заняття 3/15. Криптоаналіз сучасних блокових шифрів.** 1. Диференційний криптоаналіз. 2. Лінійний криптоаналіз.	дошка, крейда демонстр. матеріал	[2] с. 166-170.
16.	Лекція № 7	3	2	1	**Заняття 3/16. Сучасні шифри потоку.** 1. Синхронні шифрі потоку. 2. Несинхронні шифрі потоку. **Самостійна робота 10** Несинхронні шифрі потоку.	дошка, крейда демонстр. матеріал	[2] с. 171-177.
17.	Лекція № 8	3	2	1	**Заняття 3/17. Стандарт шифрування даних DES.** 1. Загальні положення DES. 2. Структура DES. 3. Функція DES. **Самостійна робота 11** Функція DES.	дошка, крейда, демонстр. матеріал	[2] с. 183-193. [25]
18.	Практичне заняття № 6	3	2	1	**Заняття 3/18. Стандарт шифрування даних DES.** 1. Приклад шифрування в DES. 2. Приклад розшифрування в DES. **Самостійна робота 13** Криптоаналіз DES.	дошка, крейда, демонстр. матеріал	[2] с. 197-199. [25]
19.	Практичне заняття № 7	3	2	1	**Заняття 3/19. Дослідження криптостійкості DES.** 1. Властивості DES. 2. Критерії розробки DES. 3. Дослідження слабості DES. **Самостійна робота 14** Дослідження слабості DES.	дошка, крейда, демонстр. матеріал	[2] с. 199-206. [25]

20.	Практичне заняття № 8	3	2	1	**Заняття 3/20. Дослідження багатократного використання DES.** 1. Двократний DES. 2. Трьохкратний DES. 3. Безпека DES. **Самостійна робота 15** Трьохкратний DES.	дошка, крейда, демонстр. матеріал	[2] с. 206-211 [25]
21.	Лекція № 9	3	2	1	**Заняття 3/21. Удосконалений стандарт шифрування AES.** 1. Загальні положення AES. 2. Структура AES. 3. Структура раунду AES. **Самостійна робота 16** Структура раунду AES.	дошка, крейда, демонстр. матеріал	[2] с. 215-219 [26]
22.	Практичне заняття № 9	3	2	1	**Заняття 3/22. Дослідження крипто-графічних перетворень AES.** 1. Підстановка. 2. Перестановка. 3. Змішування. 4. Додавання ключа. **Самостійна робота 17** Примітивні перетворень AES.	дошка, крейда, демонстр. матеріал	[2] с. 219-231 [26]
23.	Лекція № 10	3	2	1	**Заняття 3/23. Розширення ключів в AES.** 1. Розширення ключів в AES-128. 2. Розширення ключів в AES-192 і AES-256. 3. Аналіз розширення ключів в AES. **Самостійна робота 18** Аналіз розширення ключів в AES.	дошка, крейда, демонстр. матеріал	[2] с. 231-237 [26]
24.	Групове заняття № 5	2	2		**Заняття 3/24. Приклади розширення ключів в AES.** 1. Приклади знаходження ключів в AES-128. 2. Приклади знаходження ключів в AES- 192.	дошка, крейда, демонстр. матеріал	[2] с. 231-237 [26]
25.	Практичне заняття № 10	4	2	2	**Заняття 3/25. Дослідження проектів реалізації AES та його аналіз.** 1. Проекти реалізації AES. 2. Аналіз AES. **Самостійна робота 19** Реалізація AES.	дошка, крейда демонстр. матеріал	[2] с. 237-244 [26]
26.	Лекція № 11	2	2		**Заняття 3/26. Стандарт шифрування даних ДСТУ ГОСТ 28147:2009.** 1. Загальні положення ГОСТ 28147. 2. Структура алгоритму ГОСТ 28147. 3. Структура раунду ГОСТ 28147. 4. Криптоаналіз алгоритму ГОСТ 28147.	дошка, крейда, демонстр. матеріал	[1] с. 220-223, [2,5,8,11].
27.	Практичне заняття № 11	4	2	2	**Заняття 3/27. Дослідження режимів роботи ДСТУ ГОСТ 28147:2009.** 1. Режим простої заміни. 2. Режим гамування. 3. Режим гамування зі зворотним зв'язком. 4. Режим виробітки імітовставки. **Самостійна робота 20** Реалізація ДСТУ ГОСТ 28147:2009.	дошка, крейда, демонстр. матеріал	[1] с. 220-223, [2, 5, 8, 11].

28.	Групове заняття № 6	2	2		**Заняття 3/28. Стандарт шифрування даних ДСТУ 7624:2014.** 1. Загальні положення ДСТУ 7624:2014. 2. Функція шифрування.	дошка, крейда, демонстр. матеріал	[15] ДСТУ 7624:2014
29.	Практичне заняття № 12	4	2	2	**Заняття 3/29. Дослідження режимів роботи ДСТУ ГОСТ 28147:2009.** 1. Режим простої заміни. 2. Режим гамування. 3. Режим гамування зі зворотним зв'язком. 4. Режим виробітки імітовставки. **Самостійна робота 20** Реалізація ДСТУ ГОСТ 28147:2009.	дошка, крейда, демонстр. матеріал	[1] с. 220-223, [2, 5, 8, 11].
30.	Групове заняття № 7	2	2		**Заняття 3/30. Стандарт шифрування даних ДСТУ 7624:2014.** 1. Формування циклових ключів. 2. Криптографічна стійкість блокового шифру «КАЛИНА». 3. Режими роботи ДСТУ 7624:2014.	дошка, крейда, демонстр. матеріал	[15] ДСТУ 7624:2014
31.	Групове заняття № 8	3	2	1	**Заняття 3/31. Режими роботи сучасних блокових шифрів.** 1. Режим електронної кодової книги. 2. Режим зчеплення блоків шифрованого тексту. 3. Режим кодованого зворотного зв'язку. 4. Режим зовнішнього зворотного зв'язку. 5. Режим лічильника. **Самостійна робота 21** Порівняння режимів роботи сучасних блокових шифрів.	дошка, крейда, демонстр. матеріал	[2] с. 249-263
32.	Групове заняття № 9	5	2	3	**Заняття 3/32. Потокові системи шифрування.** 1. RC4. 2. A5/1. 3. Проблеми використання симетричних криптографічних систем.	дошка, крейда, демонстр. матеріал	[2] с. 263-270 [12] с. 270-282
33.	Практичне заняття № 13	4	2	2	**Заняття 3/33. Дослідження режимів роботи потокових системи шифрування.** 1. RC4. 2. A5/1. **Самостійна робота 20** Реалізація ДСТУ ГОСТ 28147:2009.	дошка, крейда, демонстр. матеріал	[1] с. 220-223, [2, 5, 8, 11].
34.	Практичне заняття № 14	4	2	2	**Заняття 3/34. Оцінка стійкості потокових системи шифрування.** 1. RC4. 2. A5/1. **Самостійна робота 20** Реалізація ДСТУ ГОСТ 28147:2009.	дошка, крейда, демонстр. матеріал	[1] с. 220-223, [2, 5, 8, 11].
35.	Групове заняття № 10	2	2		**Модульна контрольна робота.**	метод. матеріал	[1-12, 1-9].
Разом		**105**	**70**	**35**			

Семестр 7							
Змістовий модуль 4. Асиметричні криптосистеми. Геш-функції							
1.	Лекція № 1	3	2	1	**Заняття 4/1.** 1. Рейтингова система оцінювання. 2. Загальні поняття та визначення (криптографічні ґеш-функції, цифровий підпис, автентифікація об'єктів, управління ключами).	Дошка, крейда, демонстр. матеріал	[2] с. 365-499.
2.	Лекція № 2	3	2	1	**Заняття 4/2. Цілісність повідомлень.** 1. Загальні положення. 2. Криптографічні критерії ґеш-функції. 3. Випадкова модель Oracle. 4. Атаки випадкової моделі Oracle.	Дошка, крейда, демонстр. матеріал	[2] с. 365-380.
3.	Групове заняття № 1	3	2	1	**Заняття 4/3. Встановлення дійсності повідомлення.** 1. Код виявлення модифікації. 2. Код встановлення дійсності повідомлення.	Дошка, крейда, демонстр. матеріал	[2] с. 380-390.
4.	Лекція №3	3	2	1	**Заняття 4/4. Ітеративні ґеш-функції.** 1. Ітеративна ґеш-функція. Схема Меркеля-Дамгарда. 2. Підходи до розробки ґеш-функцій. 3. Схеми ґеш-функцій: Рабіна, Девіса-Мейера, Матіса-Мейера-Осеаса, Міагучи-Пренеля.	Дошка, крейда, демонстр. матеріал	[2] с. 392-395.
5.	Практичне заняття №1	3	2	1	**Заняття 4/5. Дослідження алгоритму безпечного ґешування SHA-512.** 1. Створення дайджест повідомлення SHA-512. 2. Функції розширення слова та стиску в SHA-512. 3. Загальна структура раунду SHA-512.	Дошка, крейда, демонстр. матеріал	[2] с. 396-405.
6.	Практичне заняття № 2	3	2	1	**Заняття 4/6. Дослідження ітеративної функції криптографічного ґешування Whirlpool.** 1. Загальна ідея шифру Whirlpool. 2. Структура раунду шифру Whirlpool. 3. Розширення ключа та аналіз шифру Whirpool.	Дошка, крейда, демонстр. матеріал	[2] с. 405-414.
7.	Групове заняття № 2	3	2	1	**Заняття 4/7. Стандарти функції ґешування.** 1. ДСТУ ГОСТ 34.311:2009. 2. ДСТУ 7564:2014.	Дошка, крейда, дем. мат	[16]
8.	Лекція № 4	4	2	2	**Заняття 4/8. Загальні поняття асиметрично-ключових криптосистем.** 1. Загальна ідея асиметрично-ключової криптосистеми. 2. «Лазівка» в односторонній функції. **Самостійна робота 22** Види «Лазівок» в односторонній функції.	дошка, крейда, демонстр. матеріал	[2] с. 318-323 [28,29]

9.	Групове заняття № 3	2	2	1	**Заняття 4/9. Ранцева криптосистема.** 1. Загальна ідея ранцевої криптосистеми. 2. Генерація ключів, шифрування та розшифрування в ранцевій криптосистемі. 3. Приклад використання ранцевої криптосистеми.	дошка, крейда, демонстр. матеріал	[2] с. 323-327 [27]
10.	Групове заняття № 4	2	2	1	**Заняття 4/10. Криптографічна система RSA.** 1. Загальні положення. 2. Шифрування, розшифрування та генерація ключів в RSA. 3. Приклади RSA.	дошка, крейда, демонстр. матеріал	[2] с. 327-332 [28,29]
11.	Лекція № 5	3	2	1	**Заняття 4/11. Загальні положення про цифровий підпис.** 1. Порівняння звичайного та цифрового підписів. 2. Процес цифрового підпису. 3. Послуги безпеки цифрового підпису. 4. Атаки цифрового підпису.	Дошка, крейда, демонстр. матеріал	[2] с. 419-426. [30]
12.	Групове заняття № 5	3	2	1	**Заняття 4/12. Схема цифрового підпису RSA.** 1. Загальна ідея цифрового підпису RSA. 2. Підпис RSA дайджесту повідомлення. 3. Атаки на дайджест RSA.	Дошка, крейда, демонстр. матеріал	[2] с. 427-431. [28]
13.	Практичне заняття № 3	6	4	2	**Заняття 4/13. Дослідження схем цифрових підписів.** 1. Цифровий підпис RSA. 2. Цифровий підпис Ель-Гамаля. 3. Цифровий підпис Шнорра. 4. Стандарт цифрового підпису DSS.	Дошка, крейда, демонстр. матеріал	[2] с. 427-439. [28,30]
14.	Групове заняття № 6	3	2	1	**Заняття 4/14. Дослідження схеми цифрового підпису на еліптичних кривих.** 1. Загальні положення. 2. Процедура генерації ключів. 3. Процедура підпису та перевірки.	Дошка, крейда, демонстр. матеріал	[2] с. 439-441. [30]
15.	Групове заняття № 7	3	2	1	**Заняття 4/15. Стандарти цифрового підпису.** 1. IEEE P1363. 3. ДЕРЖСТ 34.310-2012. 4. ДСТУ 4145-2002.	Дошка, крейда, демонстр. матеріал	ДЕРЖСТ 34.310 ДСТУ 4145-2002
Змістовий модуль 5. Асиметричні протоколи							
16.	Лекція №6	3	2	1	**Заняття 5/1. Автентифікація об'єкту.** 1. Загальні положення. 2. Паролі та атаки на нього. 3. Методи біометрії.	Дошка, крейда, дем. мат	[2] с. 448-468.
17.	Групове заняття № 8	3	2	1	**Заняття 5/2. Автентифікація суб'єкту.** 1. Загальні положення. 2. Класифікація схем автентифікації. 3. Методи біометрії.		
18.	Лекція №7	3	2	1	**Заняття 5/3. Автентифікація за допомогою функції "запит-відповідь".** 1. Використання симетричного шифру. 2. Використання ключового ґешування. 3. Використання асиметричного шифру.	Дошка, крейда, демонстр. матеріал	[2] с. 454-458.

					4. Використання цифрового підпису.		
19.	Групове заняття № 9	3	2	1	**Заняття 5/4. Автентифікація асиметричними методами.** 1. Використання симетричного шифру. 2. Використання ключового ґешування. 3. Використання асиметричного шифру. 4. Використання цифрового підпису.		
20.	Практичне заняття № 4	6	4	2	**Заняття 5/5. Дослідження протоколів з нульовим розголошенням.** 1. Протокол Фіата-Шаміра. 2. Протокол Фейге-Фіата-Шаміра. 3. Протокол Кіскатера-Гілу.	Дошка, крейда, демонстр. матеріал	[2] с. 460-464.
21.	Лекція №8	3	2	1	**Заняття 5/6. Управління ключами з використанням симетричного шифрування.** 1. Центр розподілу ключів (KDC). 2. Простий протокол KDC. 3. Протокол Нідхема-Шредера. 4. Протокол Отвея-Ріса.	Дошка, крейда, демонстр. матеріал	[2] с. 471-477.
22.	Групове заняття №10	3	2	1	**Заняття 5/7. Протокол встановлення достовірності Kerberos.** 1. Сервери протоколу Kerberos. 2. Дослідження протоколу Kerberos.	Дошка, крейда, демонстр. матеріал	[2] с. 477-480.
23.	Практичне заняття №5	3	2	1	**Заняття 5/8. Дослідження методів погодження симетричних ключів.** 1. Метод Діффі-Хелмана. 2. Метод ”від станції до станції“.	Дошка, крейда, демонстр. матеріал	[2] с. 480-487.
24.	Лекція №9	3	2	1	**Заняття 5/9. Управління ключами з використанням асиметричного шифрування.** 1. Центр довіри та сертифікації. Сертифікат X.509. 2. Інфраструктура відкритих ключів (PKI).		
25.	Практичне заняття №6	5	4	1	**Заняття 5/10. Управління ключами з використанням асиметричного шифрування.** 1. Центр довіри та сертифікації. Сертифікат X.509. 2. Інфраструктура відкритих ключів (PKI).	Дошка, крейда, демонстр. матеріал	[2] с. 487-497.
26.	Лекція №10	3	2	1	**Заняття 5/11. Інфраструктура відкритих ключів.** 1. ЦСК. 2. АЦСК.		
27.	Практичне заняття №7	5	4	1	**Заняття 5/12. Налаштування інфраструктури відкритих ключів.** 1. Налаштування ЦСК. 2. Налаштування АЦСК.		
28.	Лекція №11	3	2	1	**Заняття 5/13. Налаштування інфраструктури відкритих ключів II.** 1. Налаштування ЦСК. 2. Налаштування АЦСК. 3. Структура АЦСК.		
29.	Практичне заняття №8	5	4	1	**Заняття 5/14. Налаштування інфраструктури відкритих ключів I.** 1. Налаштування ЦСК.		

					2. Налаштування АЦСК.		
30.	Групове заняття № 11	3	2	1	**Модульна контрольна робота**	метод. матеріал	[1-12, 1-9].
Разом		**99**	**70**	**29**			

Умови допуску до заліку

Курсант допускається до диференційованого заліку, якщо він до початку заліку ліквідував заборгованість за всіма видами робіт, які передбачені робочим навчальним планом (робочою програмою навчальної дисципліни).

Підвищення рейтингової оцінки (в балах) курсанта з кредитного модуля відбувається за рахунок часу відведеного на самостійну роботу.

Рейтингова оцінка (в балах) з кредитного модуля має бути не менше 35 балів від суми вагових балів контрольних заходів протягом семестру.

Курсант, який набрав протягом семестру рейтингову оцінку з кредитного модуля менше за 35 балів, до диференційованого заліку не допускається. Він отримує оцінку **неприйнятно** з обов'язковим повторним вивченням навчальної дисципліни.

Курсант, який набрав протягом семестру рейтингову оцінку (в балах) з кредитного модуля від 35 до 49 балів, зобов'язаний виконати контрольне завдання.

Курсант, який набрав протягом семестру рейтингову оцінку (в балах) з кредитного модулю більше за 50 балів, має можливості:

– отримати залікову оцінку без виконання контрольного завдання ("автоматом") відповідно до набраної рейтингової оцінки (в балах);

– виконати контрольне завдання з метою підвищення оцінки.

Критерії оцінювання контрольного завдання

Максимальна кількість балів за виконання контрольного завдання ($R_{КЗ}$) дорівнює – 100:

– повна відповідь на два теоретичні питання і правильно вирішена практична задача 100;

– повна відповідь тільки на два теоретичні питання 60;

– повна відповідь тільки на одне теоретичне питання 30;

– правильно вирішена практична задача 40;

– часткова відповідь на одне теоретичне питання 15…29;

– практичну задачу вирішено не у повному обсязі 20…39;

– відповідь на теоретичне питання містить грубі помилки 1…14;

– вирішення практичної задачі містить грубі помилки 1…19;

– відсутність відповіді на теоретичні питання та неправильно вирішена практична задача 0.

Для визначення оцінки за шкалою ЄКТС та національною шкалою рейтингова оцінка (в балах) з кредитного модуля (R) за виконання контрольного завдання переводиться згідно з таблицею.

Значення R	**Оцінка за національною шкалою**

90 - 100	відмінно
80 - 89	дуже добре
65 - 79	добре
55 - 64	задовільно
50 - 54	достатньо
35-49	незадовільно
1 - 34	неприйнятно

Порядок застосування рейтингової системи оцінювання

Рейтингова система оцінювання успішності з кредитного модуля (навчальної дисципліни) доводиться курсантам на першому занятті.

Рейтингова оцінка (сума балів) з кредитного модуля, яку курсант набрав протягом семестру доводиться до курсанта на останньому занятті.

Якщо курсант набрав протягом семестру більше 50 балів та не бажає підвищувати оцінку (суму балів), то викладач записує до відомості обліку успішності рейтингову оцінку (суму балів) кредитного модуля за семестр.

Якщо курсант набрав протягом семестру більше 50 балів та бажає підвищити оцінку (суму балів), то він виконує контрольне завдання, при цьому рейтингова оцінка (сума балів) кредитного модуля за семестр скасовується і він отримує рейтингову оцінку (бали) тільки за результатом виконання контрольного завдання.

Якщо курсант за результатом виконання контрольного завдання набрав від 1 до 34 балів, то він отримує оцінку **(неприйнятно)** без можливості повторного перескладання диференційованого заліку.

Перескладання заліку проводиться за окремим розкладом.

Критерії оцінювання знань і вмінь курсанта за результатами вивчення кредитного модуля наступні

оцінка "**відмінно**" (90-100 балів) виставляється за високий рівень знань (допускаються деякі неточності) навчального матеріалу кредитного модуля, що міститься в основних і додаткових рекомендованих джерелах, вміння аналізувати явища, які вивчаються, у їхньому взаємозв'язку і розвитку, чітко, лаконічно, логічно, послідовно відповідати на поставлені запитання, вміння застосовувати теоретичні положення при розв'язанні практичних завдань;

оцінка "**дуже добре**" (80-89 балів) виставляється за знання навчального матеріалу кредитного модуля вище середнього рівня, включаючи розрахунки, аргументовані відповіді на поставлені запитання (можлива невелика кількість неточностей), вміння застосовувати теоретичні положення під час розв'язанні практичних завдань;

оцінка "**добре**" (65-79 балів) виставляється в цілому за правильне розуміння навчального матеріалу кредитного модуля, включаючи розрахунки, аргументовані відповіді на поставлені питання, які, однак, містять певні (несуттєві) недоліки, за вміння застосовувати теоретичні положення при розв'язанні практичних завдань;

оцінка "**задовільно**" (55-64 балів) виставляється за посередні знання навчального матеріалу кредитного модуля, малоаргументовані відповіді, слабке застосовування теоретичних положень під час розв'язання практичних завдань;

оцінка "**достатньо**" (50-54 балів) виставляється за слабкі знання навчального матеріалу кредитного модуля, неточні або малоаргументовані відповіді, з порушенням послідовності його викладення, за слабке застосовування теоретичних положень під час розв'язанні практичних завдань;

оцінка "**незадовільно**" (35-49 балів) з можливістю повторного складання екзамену, виставляється за незнання значної частини навчального матеріалу кредитного модуля, суттєві помилки у відповідях на питання, невміння застосовувати теоретичні положення при розв'язанні практичних завдань;

оцінка "**неприйнятно**" (1-34 балів) виставляється за незнання значної частини навчального матеріалу кредитного модуля, суттєві помилки у відповідях на запитання, невміння орієнтуватися при розв'язанні практичних завдань, незнання основних фундаментальних положень з обов'язковим повторним вивченням навчальної дисципліни.

Рекомендована література

Базова

1. *Алферов А.П., и др.* Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2001. – 480 с.

2. *Фороузан А.Б.* Криптография и безопасность сетей: Учебное пособие. – М.: 2010. – 784 с.

3. *Смець В., Мельник А., Попович Р.* Сучасна криптографія. Основні поняття. – Львів: Бак, 2003. – 144 с.

4. *Поповский В.В.* Основы криптографической защиты информации в телекоммуникационных системах. Ч. 1./В.В. Поповский, А.В. Персиков. – Х.: «Компания СМИТ», 2010. – 352 с.

5. *Поповский В.В.* Основы криптографической защиты информации в телекоммуникационных системах. Ч. 2./В.В. Поповский, А.В. Персиков. – Х.: «Компания СМИТ», 2010. – 564 с.

6. *Столингс В.* Криптография и защита сетей. Принципы и практика. – Москва. Санкт-Петербург. Киев, 2001. – 668.

7. *Шнайер Б.* Прикладная криптография 2-е издание Протоколы, алгоритмы и исходные тексты на языке С. – Издательский дом «Вильямс», 2005, – 424с.

8. *Венба М.* Современная криптография. Теория и практика. – Учебное пособие. – С.П.-М., 2005. – 760 с.

9. *Харин Ю.С.* Математические основы криптологии: Учебное пособие. – Мн.: БГУ, 1999. – 319 с.

10. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

11. *Петров А.А.* Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.: ил.

12. *Коркішко Т.*, *Мельник А., Мельник В.* Алгоритми та процесори блокового шифрування. – Львів: Бак, 2003. – 168 с.

13. *Чмора А.Л.* Современная прикладная криптография. – М.: Гелиус АРВ, 2001. - 244 с.

14. *Фомичев В.М.* Методы дискретной математики в криптологии: Курс лекций. – М.: ДИАЛОГ-МИФИ, 2010 – 422 с.

15. Національний стандарт України ДСТУ 7624:2014. Алгоритм симетричного блокового перетворення.

16. Національний стандарт України ДСТУ 7624:2014. Функція хешування.

17. *Горбенко І.Д., Горбенко Ю.І.* Прикладна криптологія: Теорія. Практика. Застосування: Монографія. – Харків: видавництво «Форт», 2012. – 880 с.

Допоміжна

18. *Шеннон К.* Работы по теории информации и кибернетике

19. *Домарев В.В.* Безопасность информационных технологий. – Москва. Санкт-Петербург. Киев, 2002 – 688 с.

20. *Рябко Б.Я. Фионов А.Н.* Криптографические методы защиты информации: Учебное пособие для вузов. – М.: Горячая линия —Телеком, 2005. — 229 с.

21. *Бабаш А.В., Шанкин Г.П.* Криптография. – М.: СОЛОН-Р, 2002. – 512 с.

22. *Брассар Ж.* Современная криптология. – М.: Полимед, 1999. – 354 с.

23. *Нечаев В.И.* Элементы криптографии. Основы теории защиты информации. - М.: Высшая школа, 1999. - 278 с.

24. *Лагун А.Е.* Криптографічні системи та протоколи: Навчальний посібник – Львів: Видавництво Львівська політехніка, 2013. – 96 с.

12. Інформаційні ресурси

25. FIPS 46-3 Data Encryption Standard (DES).

26. FIPS Pub 197, Advanced Encryption Standard (AES).

27. NIST SP 800-57 Cryptographic Key Management

28. FIPS 186-3 RSA Algorithm developed by Rivest, Shamir and Adelman.

29. ANSI X9.31 A public-key algorithm

30. FIPS 186-4 Digital Signature Standard (DSS).

Начальник кафедри ЧЕВАРДІН В.Є.

Розробник ЧЕВАРДІН В.Є.
САМОЙЛОВ І.В.
ЯКОВЛЕВ С.В.