Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«___» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «МЕТОДИ ПОБУДОВИ І АНАЛІЗУ КРИПТОСИСТЕМ»

для студентів

спеціальності	125 Кібербезпека та захист інформації
освітнього рівня	другого (магістерського)
освітньої програми	125.00.02 Безпека інформаційних і комунікаційних систем

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 1666/23
(підпис) (прізвище, ініціали)
«___» _____ 2023 р.

2023 – 2024 навчальний рік

Розробник:

Гулак Геннадій Миколайович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Гулак Геннадій Миколайович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 23.08.2023 р. № 8

Завідувач кафедри _____ (підпис) Павло СКЛАДАННИЙ

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.02 Безпека інформаційних і комунікаційних систем)

___.___. 2023 р.

Керівник освітньої програми ___ (підпис) Володимир СОКОЛОВ

Робочу програму перевірено

___.___. 2023 р.

Заступник декана _____ (підпис) Євген ІВАНІЧЕНКО

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	вибіркова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4 / 120	
Курс	2	
Семестр	3	
Кількість змістових модулів з розподілом:	2	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	32	
Модульний контроль	8	
Семестровий контроль	–	
Самостійна робота	80	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Методи побудови і аналізу криптосистем» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів другого (магістерського) рівня відповідно до навчальних планів спеціальності 125 Кібербезпека та захист інформації, освітньої програми 125.00.02 Безпека інформаційних і комунікаційних систем.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач другого (магістерського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Методи побудови і аналізу криптосистем» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Методи побудови і аналізу криптосистем» складається з 2-х змістових модулів: «Методи та задачі синтезу і аналізу криптосистем»; «Забезпечення безпеки криптографічного захисту в комп’ютерних системах і мережах». Обсяг дисципліни – 120 год (4 кредити).

Метою викладання навчальної дисципліни «Методи побудови і аналізу криптосистем» є отримання компетентностей в області побудови і аналізу криптосистем для захисту інформації в комп’ютерних мережах.

Завдання:

- надання студентам теоретичних знань про задачі та особливості криптографічного захисту інформації у комп’ютерних мережах.
- формування у студентів категоріальних понять з основ математики побудови і аналізу симетричних та асиметричних криптографічних перетворень;
- формування у студентів умінь безпечно керувати ключами на основі кращих світових практик;
- стимулювання студентів до активної аналітико-пошукової роботи, що спрямована на визначення ефективних шляхів розвитку у сфері захисту інформації.

У результаті вивчення навчальної дисципліни формуються загальні компетентності:

- ***компетентності у сфері навчання:***
  - здатність до організації самостійної навчальної, практичної та науково-дослідної діяльності;
- ***компетентності у сфері застосування знань в практичних ситуаціях***
  - вміння застосовувати здобуті теоретико-концептуальні професійні знання у процесі практичної, викладацької та науково-дослідної роботи;

фахові компетентності:

ФК-8: здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

3. Результати навчання за дисципліною

За результатами вивчення курсу «Методи побудови і аналізу криптосистем» студенти повинні

знати:

- вимоги нормативно-правових актів, що визначають порядок криптографічного захисту інформації;
- джерела загроз безпеки криптосистем, вразливості криптосистем і методи їх блокування та нейтралізації;
- основні методи та принципи побудови, досліджень і безпечного застосування криптосистем для захисту інформаційних ресурсів комп'ютерних систем і мереж;
- основні стандартні криптографічні протоколи сучасних комп'ютерних систем і мереж, застосування криптографічних примітивів типових операційних систем;
- принципи побудови та проєктування стаціонарних і мобільних мереж спеціального зв'язку, систем надання електронних довірчих послуг.

уміти:

- працювати з концептуальними моделями симетричних та асиметричних криптосистем, систем генерації, розподілу та управління криптографічними ключами, застосовувати криптографічні функції в системах автентифікації і ідентифікації суб'єктів і об'єктів комп'ютерних систем і мереж, захисту конфіденційності, цілісності та авторства;
- визначати необхідні види та рівні захисту сучасних засобів криптографічного захисту інформації;
- створювати засобами стандартних операційних систем елементи захисту інформації та досягти наступних **програмних результатів навчання:**

РН-3: провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі;

РН-4: застосовувати, інтегрувати, розробляти, впроваджувати, удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки;

РН-13: досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна робота
		Лекції	Семінари	Практичні	Лабораторні	Модульний контроль	
Змістовий модуль 1. Методи та задачі синтезу і аналізу криптосистем							
Тема 1. Проблеми теорії і практики побудови криптосистем	6	2		2			10
Тема 2. Операції з шифрами по Шеннону. Аналіз і синтез криптоалгоритмів. Моделі загроз безпеки криптосистем	8	2		2			10
Тема 3. Архітектура блокових і потокових шифрів та особливості їх застосування	8	2		2			10
Тема 4. Захист від маніпуляцій в комп'ютерних мережах. Процедури електронного підпису	8	2		2			10
Модульний контроль	4					4	
Разом	6**0**	8		8		4	40
Змістовий модуль 2. Забезпечення безпеки криптографічного захисту в комп'ютерних системах і мережах							
Тема 5. Криптографічний захист в комунікаційних протоколах	8	2		2			10
Тема 6 Методи управління безпекою ключів в комп'ютерних системах	8	2		2			10
Тема 7. Архітектура системи електронних довірчих послуг	8	2		2			10
Тема 8. Технології блокчейн	8	2		2			10
Модульний контроль	4					4	
Разом	60	8		8		4	40
Усього	120	16		16		8	80

5. Програма навчальної дисципліни

Змістовий модуль 1. Методи та задачі синтезу і аналізу криптосистем

Тема 1. Проблеми теорії і практики побудови криптосистем

Предмет, мета і завдання, структура дисципліни. Базові поняття у галузі криптографічного захисту інформації (КЗІ). Сутність симетричних та асиметричних криптосистем, обєкти дослідження. Симетричне шифрування, цифровий конверт, цифровий підпис. Поняття про методи криптоаналіза: частотний аналіз, впорядкування ключів. Практичні вимоги до криптосистем.

Тема 2. Операції з шифрами по Шеннону. Аналіз і синтез криптоалгоритмів. Модель загроз та модель порушника

Властивості шифрів та безпека їх застосування: блокові та потокові шифри, попереднє шифрування та лінійне засекречування. Операції з шифрами по Шеннону. Теорема Маркова. Властивості елементарних шифрів (заміна, перестановка, Хілла, Вернама, Віжинера) що

впливають на безпеку складеної системи. Приклади комбінацій елементарних шифрів в стандартах криптографічних перетворень. Етапи життєвого циклу засобів КЗІ та їх характеристика. Криптосхема засобу КЗІ. Модель загроз та модель порушника. Види атак на криптосистеми.

Тема 3. Архітектура блокових та потокових шифрів та режими їх застосування.

Основні елементи рекурентних схем: регістри зсуву, двійкові функції. Характеристика основних елементів шифру на основі рекурентних схем та їх властивості. Принципи побудови криптоалгоритмів за схемами Файстеля і «квадрат», порівняння стандартів ДСТУ 7624-2014, AES. Характеристика режимів роботи блокових алгоритмів ECB, CBC, CFB, OFB в засобах КЗІ.

Тема 4. Захист від маніпуляцій в комп'ютерних мережах. Процедури електронного підпису (ЕП).

Загрози маніпуляцій у кіберпросторі. Поняття імітостійкості шифру. Принципи побудови та застосування функцій хешування. Формування та застосування кодів автентифікації повідомлень (MAC) для контролю цілісності. Види ЕП, механізми формування та перевіряння кваліфікованого ЕП із застосуванням асиметричних алгоритмів (RSA, DSA, Ель Гамаля, ECDS). Криптографічні примітиви в операційних системах Windows.

<u>Змістовний модуль 2</u>. Забезпечення безпеки криптографічного захисту в комп'ютерних системах і мережах

Тема 5. Криптографічний захист в комунікаційних протоколах

Поняття телекомунікаційного протоколу. Застосування криптографічних протоколів: автентифікація, розподіл ключів, підтвердження автентичності, захист цілісності і конфіденційності (RADIUS, IPSec, SSL/TLS, HTTPS, VPN). Методи автентифікації абонентів мереж спеціального зв'язку з використанням симетричних та асиметричних криптосистем. Стандарти захищених протоколів в мережі Інтернет.

Тема 6. Методи управління безпекою ключів в комп'ютерних системах

Характеристика етапів життєвого циклу криптографічних ключів. Особливості генерації та тестування ключової інформації. Безпека генераторів випадкових і псевдовипадкових чисел. Поняття про генерацію простих чисел для асиметричних криптосистем.

Тема 7. Архітектура системи електронних довірчих послуг (ЕДП).

Вимоги законодавства щодо побудови системи ЕДП: акредитований центр сертифікації ключів, передача документованої інформації, відмітка часу. Стандарт сертифікату відкритого ключу X.509.

Тема 8. Технології блокчейн

Механізми формування та перевіряння в технології блокчейн. Особливості безпеки блокчейн

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, екзамен.
- *Комп'ютерного контролю:* тестові програми.

- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	4	4	4	4
Відвідування семінарських занять					
Відвідування практичних занять	1	4	4	4	4
Відвідування лабораторних занять					
Робота на семінарському занятті					
Робота на практичному занятті	10	4	40	4	40
Лабораторна робота (в тому числі допуск, виконання, захист)					
Виконання завдань для самостійної роботи	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25
Виконання ІНДЗ					
Разом			78		78
Максимальна кількість балів: 156					
Розрахунок коефіцієнта: 156/100=1,56					

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Методи і задачі синтезу і аналізу криптосистем		40	5
1	Тема 1. Проблеми теорії і практики побудови криптосистем Тема 2. Операції з шифрами по Шеннону. Аналіз і синтез криптоалгоритмів. Модель загроз та модель порушника Тема 3. Архітектура блокових шифрів та режими їх застосування Тема 4. Процедури електронного підпису	40	5
Змістовий модуль 2. Забезпечення безпеки криптографічного захисту в комп'ютерних системах і мережах		40	5
2	Тема 5. Криптографічний захист в комунікаційних протоколах Тема 6. Методи управління безпекою ключів в комп'ютерних системах Тема 7. Архітектура систем електронних довірчих послуг Тема 8. Технології блокчейн	40	5
	Разом	80	8

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	1 бал
2	Доказовість висновків, обгрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бал
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	4 бали

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – комп'ютерний тест, що складається 20 запитань закритої та відкритої форм.

Модульна контрольна робота оцінюється у 20 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі заліку, умовою отримання якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Питання для самоконтролю

1. Зміст та задачі криптографії, криптоаналізу та криптології.
2. Зміст та завдання криптографічного захисту інформації (КЗІ).
3. Об'єкти досліджень у криптографії
4. Властивості інформації, що підлягають захисту за допомогою криптографії.
5. Визначення термінів зашифрування, розшифрування, дешифрування, рівняння криптоперетворення у загальному вигляді. Сутність криптоаналізу.
6. Елементарні шифри та їх властивості: проста заміна, перестановка, шифри Вернама, Віжинера, Хілла.
7. Практичні вимоги до шифрів, поняття стійкості криптографічного перетворення.

8. Визначення криптосистеми, види реалізації засобів КЗІ та їх характеристика.
9. Схема секретного зв’язку по Шеннону.
10. Характеристика моделі порушника безпеки КЗІ.
11. Класи безпеки засобів КЗІ та їх характеристика.
12. Загальна структурна схема (складові) засобу КЗІ.
13. Визначення та властивості потокових і блокових шифрів.
14. Поняття поширення шифром помилок, формулювання та значення теореми Маркова.
15. Рівняння криптоперетворення у загальному вигляді, визначення та застосування симетричних та асиметричних криптосистем.
16. Застосування асиметричних криптосистем для розподілу ключів.
17. Побудова схеми «цифровий конверт» за допомогою асиметричних криптосистем.
18. Визначення поняття електронний цифровий підпис, рівняння його формування та перевірки у загальному вигляді.
19. Операції з шифрами по Шеннону: добуток та зважене додавання.
20. Порядок провадження діяльності у галузі КЗІ.
21. Закони України що визначають особливості та порядок здійснення КЗІ.
22. Вимоги Указу Президента України від 1998 року № 505 щодо КЗІ.
23. Основні функції та завдання державних органів що беруть участь у реалізації політики із захисту інформації.
24. Елементи потокових шифрів: двійкові функції, комутатори, регістри зсуву.
25. Принцип Керкхофса безпеки криптографічних систем.
26. Поняття практичної та теоретичної стійкості криптосистем.
27. Види атак на криптосистеми залежно від вихідних даних.
28. Забезпечення безпеки криптографічних ключів на стадіях їх життєвого циклу.
29. Методи генерації якісних криптографічних ключів.
30. Характеристика видів криптографічних ключів залежно від ї призначення: майстер-ключі, ключі шифрування ключів, сеансові ключі.
31. Поняття про термін дії ключу, характеристика умов його визначення.
32. Оцінка стійкості шифру за методом повного перебору ключів у випадку двійкового ключу.
33. Характеристика стадій життєвого циклу засобів КЗІ: формування вихідних вимог, проектування, випробування, державна експертиза.
34. Засоби попереднього шифрування та лінійного засекречування, їх застосування.
35. Основні складові забезпечення безпеки засобів КЗІ.
36. Криптоперетворення (елементи) блокових шифрів.
37. Принципи реалізації схеми Файстеля та схеми «квадрат» для побудови блокових шифрів.
38. Режими шифрування блокових алгоритмів: ECB, CBC та їх характеристика.
39. Режими шифрування блокових алгоритмів: CFB, OFB та їх характеристика.
40. Властивості та застосування хешфункцій.
41. Призначення коду автентифікації повідомлень (MAC), його формування за допомогою блокового шифру.
42. Призначення хешфункції та її формування за допомогою блокового шифру.
43. Схема ЕЦП на основі асиметричного алгоритму RSA .
44. Асиметричне шифрування за допомогою криптосистеми RSA.
45. Принцип побудови ЕЦП на основі еліптичних кривих.
46. Визначення та застосування криптографічних протоколів.
47. Протокол Диффі-Хеллмана формування сеансового (спільного) ключу.
48. Поняття комплексної системи захисту інформації для безпеки КЗІ.
49. Принципи побудови стаціонарних мереж спеціального зв’язку.
50. Методи шифрування «лінія за лінією» та «із кінця в кінець» та їх характеристика.
51. Основні елементи та характеристика систем мобільного транкінгового зв’язку.
52. Побудова та функціонування алгоритму шифрування у системі GSM зв’язку A5/1.
53. Модель загроз для системи електронного документообігу.

54. Основні функції та завдання органів державного регулювання у сфері електронних довірчих послуг та електронної ідентифікації
55. Основні функції та завдання центрального засвідчувального органу у сфері електронних довірчих послуг.
56. Основні функції та завдання засвідчувального центру у сфері електронних довірчих послуг .
57. Основні функції та завдання кваліфікованих надавачів електронних довірчих послуг.
58. Призначення та структура сертифікату відкритого ключу.
59. Напрями реалізації державної політики у сфері КЗІ.
60. Провідні світові інституції з питань стандартизації, їх характеристика.

Шкала відповідності оцінок

Рейтингова оцінка	**Сума балів за всі види навчальної діяльності**	**Значення оцінки**
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов’язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов’язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов’язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична карта дисципліни

Разом:120 год., лекції –16 год., практичні заняття – 16 год., модульний контроль – 8 год., самостійна робота – 80 год.

Модулі (назви, бали)	**Змістовий модуль 1. Методи і задачі синтезу і аналізу криптосистем** (78 балів)				**Змістовний модуль 2. Забезпечення безпеки криптографічного захисту в комп'ютерних системах і мережах** (78 балів)			
Лекції (теми, бали)	Тема 1. Проблеми теорії і практики побудови криптосистем Аналіз і синтез криптоалгоритмів (1 бал)	Тема 2. Операції з шифрами по Шеннону. Модель загроз (1 бал)	Тема 3. Архітектура та режими блокових шифрів (1 бал)	Тема 4. Процедури електронного підпису (1 бал)	Тема 5. Криптографічний захист в комунікаційних протоколах (1 бал)	Тема 6. Методи управління безпекою ключів в комп'ютерних системах (1 бал)	Тема 7. Технології блокчейн (1 бал)	Тема 8.. Архітектура системи електронних довірчих послуг (1 бал)
Практичні заняття (теми, бали)	Властивості елементарних шифрів (11 балів)	Операції з шифрами (11 балів)	Оцінка властивостей навчального блокового шифр (11 бал)ів	Криптоаналіз шифру RSA (11 балів)	Протокол генерації ключів (11 балів)	Тестування ключів і оцінка їх безпеки (11 балів)	Аналіз навчального шифру А5/1 (11 балів)	Стандарт сертифікату відкритого ключу (11 бал.)
Самостійна робота	Самостійна робота (5 балів)				Самостійна робота (5 балів)			
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)				Модульна контрольна робота 2 (25 балів)			
Підсумковий контроль (вид, бали)	Залік							

8. Рекомендовані джерела

Основна:

1. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації: підручник/ - Вінниця: ВНТУ, 2011. – 199с.

2. Гулак Г.М. Моделювання на етапі оцінки безпеки шифраторів конфіденційної інформації // Сучасна спеціальна техніка», 2011, № 1(24), С. 73-81

3. Бурячок В.Л., Гулак Г.М., Толубко В.Л. Інформаційний та кібернетичний простори: проблеми безпеки, методи та засоби боротьби Підручник. – К.: ТОВ «СІК ГУП Україна», 2015. – 449 с.

Додаткова:

1. Гулак Г., Бурячок В., Складанний П. та ін. (2020). Криптовірологія: загрози безпеки гарантоздатним інформаційним системам і заходи протидії шифрувальним вірусам. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 6–28. https://doi.org/10.28925/2663-4023.2020.10.628
2. Гулак Г., Жданова Ю., Складанний П., та ін. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об’єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158
3. Закон України "Про інформацію" від 02.10.1992 № 2657-XII.
4. Про Державну службу спеціального зв'язку та захисту інформації України Закон України від 23.02.2006 № 3475-IV
5. Про державну таємницю Закон України від 21.01.1994 № 3855-XII
6. Про електронні довірчі послуги Закон України від 5.10.2017 № 2155-VIII
7. Про затвердження Технічного регламенту засобів криптографічного захисту інформації. Постанова Кабінету Міністрів України від 21.10.2020 р. № 991
8. Про захист інформації в інформаційно-комунікаційних системах Закон України від 05.07.1994 № 80/94-ВР.
9. Про Національну систему конфіденційного зв'язку Закон України від 10.01.2002 № 2919-III
10. Про Положення про порядок здійснення криптографічного захисту інформації в Україні Указ Президента України від 22.05.1998 № 505/98

9. Інформаційні ресурси

1. http://uk.wikipedia.org – Вікіпедія – Вільна енциклопедія
2. http://www.crypton.ua/index.php/ – Криптон: понад 20 років досвіду розробки засобів криптографічного захисту інформації
3. http://www.tritel.ua/index.php/ – Трител - Засоби КЗІ та спеціального зв’язку
4. http://www.iit.com.ua - Інститут інформаційних технологій: Інтеграція засобів криптографічного захисту інформації