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

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНФРАСТРУКТУРА ВІДКРИТИХ КЛЮЧІВ»

для студентів
спеціальності 125 Кібербезпека
освітнього рівня першого (бакалаврського)
освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем

2023 – 2024 навчальний рік

Розробник:

Киричок Роман Васильович, доктор філософії з кібербезпеки, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Киричок Роман Васильович, доктор філософії з кібербезпеки, доцент 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 01.09.2022 р. № 12

Завідувач кафедри _____ Павло СКЛАДАННИЙ

(підпис)

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.

Керівник освітньої програми _____ Артем ПЛАТОНЕНКО

(підпис)

Робочу програму перевірено

___.___. 2022 р.

Заступник декана _____ Євген ІВАНІЧЕНКО

(підпис)

Пролонговано:

на 2023/2024 н.р. _____ (Складанний П.В.), «23» 08 2023 р., протокол № 8

(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	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	6 / 180	
Курс	4	
Семестр	8	
Кількість змістових модулів з розподілом:	2	
Обсяг кредитів	6	
Обсяг годин, в тому числі:	180	
Аудиторні	70	
Модульний контроль	10	
Семестровий контроль	30	
Самостійна робота	70	
Форма семестрового контролю	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Інфраструктура відкритих ключів» є нормативним документом Київського столичного університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека та захист інформації.

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

Програма визначає обсяги знань, якими повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Інфраструктура відкритих ключів» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Інфраструктура відкритих ключів» складається з двох змістовних модулів: Основи побудови та застосування інфраструктури відкритих ключів; Практичні аспекти розгортання системи ІВК та забезпечення її функціонування. Обсяг дисципліни – 180 год. (6 кредитів).

Метою викладання навчальної дисципліни «Інфраструктура відкритих ключів» є:

– опанування загальними основами методології створення та аналізу різноманітних типових технологій побудови інфраструктури відкритих ключів;

– ґрунтовне ознайомлення студентів із основними нормативними документами в галузі інфраструктури відкритих ключів та особливостями їх застосування на практиці;

– опанування навичками проектування, впровадження та супроводу базових варіантів архітектури інфраструктури відкритих ключів;

– ознайомлення з основними підходами та технологічними рішеннями направленими на забезпечення інформаційної безпеки інфраструктури відкритих ключів.

Завдання полягає у:

– наданні студентам базових теоретичних знань у галузі інфраструктури відкритих ключів;

– наданні студентам базових знань щодо архітектури інфраструктури відкритих ключів при створенні безпечних інформаційних систем та процесів підтвердження їх відповідності;

– набутті студентами практичних навичок застосування сучасних технологій створення та

експлуатації інфраструктури відкритих ключів;

– вивченні основних принципів забезпечення інфраструктури відкритих ключів;

та набутті наступних ***фахових компетентностей:***

КФ-12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної та/або кібербезпеки.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студенти повинні

знати:

– загальні засади правового регулювання електронних довірчих послуг;

– основи забезпечення правового режиму електронного цифрового підпису;

– основні вітчизняні нормативні документи в галузі захисту інформації та міжнародні стандарти з інформаційної безпеки, процеси які висуваються ними при побудові захищених систем, особливості підтвердження відповідності побудованого захисту;

– принципи побудови систем забезпечення інформаційної безпеки;

– основні типи, призначення та характеристики технологічних рішень, направлених на забезпечення інформаційної безпеки.

уміти:

– розробляти та визначати загальні принципи побудови інфраструктури відкритих ключів, завдання, вихідні дані та фактори, які необхідно врахувати при проектуванні інфраструктури;

– здійснювати аналіз та оцінку параметрів інфраструктури відкритих ключів;

– здійснювати аналіз організаційної структури і взаємозв'язків елементів інфраструктури відкритих ключів: формувати опис інфраструктури та середовища її функціонування, визначити склад потрібного апаратного та програмного забезпечення, здійснити аналіз потрібних технологій обробки інформації, аналіз складу та характеристик елементів інфраструктури;

– здійснювати аналіз та формування політики безпеки елементів інфраструктури відкритих ключів: визначити основні складові політики безпеки, розробляти систему документів, що забезпечують реалізацію політики безпеки, визначити гарантії правильності реалізації політики безпеки та її забезпечення;

– здійснювати формування базових положень політики безпеки, розробляти правила забезпечення інформаційної безпеки;

– здійснювати оцінку ефективності систем захисту елементів інфраструктури відкритих ключів;

– застосовувати національні та міжнародні стандарти при аналізу та розробленні інфраструктури відкритих ключів та (або) її елементів;

– застосовувати типові підходи до проектування та налагодження сучасних інфраструктур відкритих ключів, здійснити порівняння підходів до організації типових інфраструктур;

– оцінювати ефективність впровадження перспективних засобів та систем захисту технологій, що використовується при створенні інфраструктури відкритих ключів;

– використовувати на практиці нормативні документи в галузі захисту інформації та міжнародні стандарти з інформаційної безпеки, розуміти відмінності побудованих відповідно до їх вимог систем;

– реалізовувати організаційні та технічні завдання, які виникають в процесі побудови інфраструктури відкритих ключів;

та досягти наступних ***програмних результатів навчання:***

ПРз-10	- аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації; - аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації; - виявляти небезпечні сигнали технічних засобів; - вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами; - визначити ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик IT та SMART-систем відповідно до вимог нормативних документів системи технічного захисту інформації; - обґрунтувати можливість створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; - впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Основи побудови та застосування інфраструктури відкритих ключів							
Тема 1. Вступ до навчальної дисципліни «Інфраструктура відкритих ключів»	20	4		6			10
Тема 2. Нормативно-правове регулювання захисту інформації в інформаційних системах, надання електронних довірчих послуг ключів	16	2		6			8
Тема 3. Міжнародні та національні стандарти щодо функціонування ІВК та забезпечення її безпеки	14	2			4		8
Тема 4. Концепція довіри при реалізації технології ІВК	20	2		4	4		10
Тема 5. Регламент суб'єктів ІВК та політика безпеки	12	4					8
Модульний контроль	6						
Разом	**88**	**14**		**16**	**8**		**44**

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 2. Практичні аспекти розгортання системи ІВК та забезпечення її функціонування							
Тема 6. Основні компоненти, сервіси та архітектури ІВК	12	2			4		6
Тема 7. Проєктування, розгортання та практичне застосування ІВК	46	6		8	12		20
Модульний контроль	4						
Разом	**62**	**8**		**8**	**16**		**26**
Семестровий контроль	30						
Усього годин	**180**	**22**		**24**	**24**		**70**

5. Програма навчальної дисципліни

Змістовий модуль 1. Основи побудови та застосування інфраструктури відкритих ключів

Тема 1. Вступ до навчальної дисципліни «Інфраструктура відкритих ключів». Сутність симетричних та асиметричних криптосистем. Цифровий конверт. Цифровий підпис. Практичні вимоги до криптографічних систем захисту інформації. Генерація та управління ключами. Накопичення (зберігання) ключів. Розподіл ключів. Життєвий цикл криптографічних ключів. Практичні вимоги та рекомендації щодо забезпечення безпеки криптографічних ключів. Поняття про модель порушника безпеки криптосистем. Модель загроз та практична стійкість криптосистем. Принцип Керкхоффса щодо безпеки шифрів та основні види атак. Класифікація криптоатак. Державна класифікація засобів КЗІ за рівнями безпеки.

Тема 2. Нормативно-правове регулювання захисту інформації в інформаційних системах, надання електронних довірчих послуг. Підходи ЄС щодо захисту інформації та електронного цифрового підпису. Правове регулювання електронних довірчих послуг в України. Терміни Закону України «Про електронні довірчі послуги (ЕДП)». Суб'єкти та склад електронних довірчих послуг. Державне регулювання у сферах електронних довірчих послуг та електронної ідентифікації. Правове регулювання захисту інформації в інформаційно-телекомунікаційних системах. Нормативні акти КМ України щодо захисту інформації в ІТС та ЕДП.

Тема 3. Міжнародні та національні стандарти щодо функціонування ІВК та забезпечення її безпеки. Основні органи зі стандартизації у галузі ІВК. Класифікація стандартів ISO/IEC, ITU-T, IEEE, ISOC у галузі ІВК. Взаємодія стандартів в галузі ІВК. Узагальнена характеристика напрямків стандартизації в галузі ІВК. Призначення сертифікату відкритого ключа та його структура за стандартом X.509.

Тема 4. Концепція довіри при реалізації технології ІВК. Поняття довіри в контексті електронних комунікацій. Політика довіри. Концепція довіри в ІВК. Ієрархічні моделі довіри. Моделі розподіленої довіри. Механізм крос-сертифікації. Концепція взаємного розпізнавання. Список довіри до сертифікатів. Концепція сертифіката акредитації.

Тема 5. Регламент суб'єктів ІВК та політика безпеки. Політика безпеки і способи її реалізації. Політика застосування сертифікатів. Ідентифікатори об'єктів. Регламент засвідчувального центру. Етапи розробки політики застосування сертифікатів. Набір положень

політики ІВК (опис загальних положень, опис спеціальних розділів). Труднощі розробки політики та регламенту. Коротка характеристика політики ІВК.

Змістовий модуль 2. Основи побудови та застосування інфраструктури відкритих ключів

Тема 6. Основні компоненти, сервіси та архітектури ІВК. Основні компоненти ІВК та їх характеристики. Основні сервіси ІВК та їх характеристика. Основні типи архітектури ІВК.

Тема 7. Проєктування, розгортання та практичне застосування ІВК. Попередній етап розгортання ІВК. Проєктування ІВК. Створення прототипу, пілотний проект і впровадження. Підготовка системи ІВК до роботи. Управління сертифікатами і ключами. Реагування на інциденти під час функціонування ІВК. Процедура анулювання цифрових сертифікатів. Відновлення, резервне копіювання та зберігання ключів в архіві. Проблеми інтеграції ІВК. Проблеми функціональної сумісності продуктів різних постачальників. Проблеми репозиторія. Практичне застосування технології ІВК. Забезпечення строгої аутентифікації. Веб-PKI на базі X.509. Перевірка сертифікатів в браузерах. Різновиди SSL-сертифікатів. Організація захищеного обміну електронною поштою. S/MIME та система PGP. Організація віртуальних приватних мереж (VPN). Система захищених електронних транзакцій SET. Проблеми вибору постачальника технології або окремих сервісів ІВК. Визначення критеріїв вибору постачальника.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної 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:* програми - емулятори.

– *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.

6.1. 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	7	7	4	4
Відвідування семінарських занять	1				
Відвідування практичних занять	1	8	8	4	4
Відвідування лабораторних занять	1	4	4	8	8
Робота на семінарському занятті	10				
Робота на практичному занятті	10	8	80	4	40
Лабораторна робота (в тому числі допуск, виконання, захист)	10	4	40	8	80
Виконання завдань для самостійної роботи	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25
Виконання ІНДЗ	30				
Разом		-	169	-	166
Максимальна кількість балів: 335					
Розрахунок коефіцієнта: 335/60=5,58					

6.2. 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. Основи побудови та застосування інфраструктури відкритих ключів		**44**	**5**
1	Вступ до навчальної дисципліни «Інфраструктура відкритих ключів»	10	1
2	Нормативно-правове регулювання захисту інформації в інформаційних системах, надання електронних довірчих послуг ключів	8	1
3	Міжнародні та національні стандарти щодо функціонування ІВК та забезпечення її безпеки	8	1
4	Концепція довіри при реалізації технології ІВК	10	1
5	Регламент суб’єктів ІВК та політика безпеки	8	1
Змістовий модуль 2. Практичні аспекти розгортання системи ІВК та забезпечення її функціонування		**26**	**5**
6	Основні компоненти, сервіси та архітектури ІВК	6	2
7	Проєктування, розгортання та практичне застосування ІВК	20	3
	Разом	**70**	**10**

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.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	**5 балів**

6.3. 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 – тест, що складається із 14 тестових завдань (відкритої та закритої форм). Модульна контрольна робота оцінюється у 25 балів.

6.4. Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі екзамену, умовою допуску до якого є отриманням студентом 35 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Форма проведення екзамену – тестування в середовищі Moodle. Екзамен оцінюється у 40 балів (32 тестових завдання відкритої та закритої форм). Оцінювання результатів засвоєння теоретичних знань та оцінювання сформованості практичних навичок володіння цифровими технологіями студентами, продемонстровані на екзамені, представлене у таблиці.

Підсумкова кількість балів (max - 40)	Оцінка за 4-бальною шкалою
1 – 23	«незадовільно»
24 – 29	«задовільно»
30 – 35	«добре»
36 – 40	«відмінно»

6.5. Орієнтовний перелік питань для семестрового контролю

1. Ключова система, як ядро будь-якої криптографічної підсистеми захисту інформації.
2. Основні задачі захисту інформації, які вирішуються шляхом використання криптографічних перетворень.
3. Базові характеристики будь-яких криптографічних методів захисту інформації.
4. Основні криптографічні процедури.
5. Загальноприйняті вимоги до сучасних криптографічних систем захисту інформації.
6. Основні аспекти симетричної криптографії. Переваги та недоліки.
7. Основні аспекти криптографії з відритим ключем. Переваги та недоліки.
8. Основні симетричні криптографічні алгоритми. Короткий опис, приклади алгоритмів та їх застосування.
9. Основні асиметричні криптографічні алгоритми. Короткий опис, приклади алгоритмів

та їх застосування.

10. Криптографічні методи забезпечення цілісності інформації та автентичності.
11. Цифровий підпис – визначення, застосування, приклади використання.
12. Генерація та управління ключами. Накопичення (зберігання) ключів.
13. Розподіл та розповсюдження ключів. Технології, методи, особливості.
14. Основні етапи життєвого циклу криптографічних ключів.
15. Практичні вимоги та рекомендації щодо забезпечення безпеки криптографічних ключів.
16. Поняття про моделі порушника безпеки, загроз та практичної стійкості криптосистем.
17. Принцип Керкхофса щодо безпеки криптографічних шифрів.
18. Інфраструктура відкритих ключів – визначення, застосування, приклади використання.
19. Хеш-функції. Визначення, загальні параметри, властивості, приклади використання.
20. Алгоритм MD 5.Опис, застосування, переваги та недоліки.
21. Стандарти хеш-функції SHA-2. Опис, застосування, переваги та недоліки.
22. Стандарт ГОСТ Р 34.11-2012. Опис, застосування, переваги та недоліки.
23. Схеми підпису електронного документа на основі асиметричних алгоритмів.
24. Основні стандарти асиметричних криптографічних алгоритмів формування та перевірки ЕЦП.
25. MITM-атака (атака людина посередині), визначення та приклад.
26. Поняття електронних довірчих послуг.
27. Основні аспекти нормативно-правового регулювання надання електронних довірчих послуг.
28. Поняття довіри та концепція довіри в ІВК.
29. Модель суворої ієрархії засвідчувальних центрів.
30. Модель розподіленої довіри
31. Ієрархії на основі політик
32. Нестрога ієрархія засвідчувальних центрів.
33. Роль цифрових сертифікатів у забезпечення безпеки застосування ЕЦП.
34. Нормативно-правова база України щодо ЕЦП.
35. Оцінка стану нормативного регулювання ЕЦП.
36. Базова архітектура ІВК та основні її характеристики.
37. Основні компоненти ІВК та короткий опис.
38. Ієрархічна модель довіри в ІВК.
39. Концепція крос-сертифікації.
40. Сервіси, що базуються на ІВК. Перелік, Опис, призначення.
41. Сертифікат відкритого ключа. Форми, складові.
42. Список відкликаних сертифікатів. Призначення. Формат. Основні складові.
43. Засвідчувальний центр. Призначення, завдання, застосування.
44. Реєстраційний центр. Призначення, завдання, застосування.
45. Репозіторій сертифікатів. Призначення, завдання, застосування.
46. Архів сертифікатів. Призначення, завдання, застосування.
47. Приклади практичного застосування ІВК.
48. Забезпечення механізму строгої аутентифікації з використанням ІВК.
49. Веб-ІВК на базі X.509.
50. Захищена система доменних імен.
51. Система захищеної електронної пошти.
52. Віртуальні приватні мережі з використанням ІВК.
53. Система захищених електронних транзакцій.
54. Етапи розгортання ІВК.
55. Основні проблеми реалізації ІВК.
56. Політики, регламент та процедури ІВК.

6.6. 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 картка дисципліни

Разом: 180 год., лекції – 22 год., практичні заняття – 24 год., лабораторні заняття – 24 год., модульний контроль – 10 год., семестровий контроль – 30 год., самостійна робота – 70 год.

Модулі (назви, бали)	**Змістовий модуль 1. Основи побудови та застосування інфраструктури відкритих ключів (169 балів)**								**Змістовий модуль 2. Практичні аспекти розгортання системи ІВК та забезпечення її функціонування (166 бали)**			
Лекції (теми, бали)	Особливості криптографічного захисту в інформаційних системах (1 бал)		Загрози безпеці криптосистем (1 бал)	Законодавство про захист інформації та електронні довірчі послуги (1 бал)		Стандарти про об'єкти ІВК, та забезпечення її безпеки (1 бал)	Концепція довіри при реалізації технології ІВК (1 бал)	Політики, регламент та процедури ІВК (2 бали)	Основні компоненти, сервіси та архітектури ІВК (1 бал)	Проєктування та розгортання інфраструктури відкритих ключів (1 бал)	Основні проблеми реалізації та ризики технології ІВК (1 бал)	Практичне застосування та проблеми вибору постачальника технології або сервісів ІВК (1 бал)
Лабораторні заняття (теми, бали)						Дослідження структури сертифікату відкритого ключа за стандартом X.509 (22 бали)	Дослідження процедур підпису електронного документу та перевірки ЕЦП (22 бали)		Побудова та застосування ІВК на основі моделі довіри, сконцентрованої навколо користувача (22 бали)	Проєктування корпоративної ІВК, побудова та валідація шляхів сертифікації (22 бали)	Підготовка пілотного проєкту корпоративної ІВК: розгортання засвідчувальних центрів та формування ієрархії (22 бали)	Тестування пілотного проєкту корпоративної ІВК та її впровадження (22 бали)
Практичні заняття (теми, бали)	Елементарні шифри та їх частотний аналіз (11 балів)	Композиція шифрів (11 балів)	Оцінка практичної стійкості криптосистем (11 балів)	Генерація випадкових бітових ключів та оцінка їх якості (22 бали)	Двійкові функції та LFSR в криптографії (11 балів)		Криптографічна хеш-функція, як механізм забезпечення цілісності інформації (22 бали)			Побудова корпоративної ІВК: попередній етап (44 бали)		
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)	Екзамен (40 балів)											

8. Рекомендовані джерела

Основна (базова):

1. Про інформацію: Закон України від 15.06.2022 № 2657-XII.
2. Про національну безпеку України: Закон України від 15.06.2022 № 2469-VIII.
3. Про захист інформації в автоматизованих системах: Закон України від 04.07.2020 № 80/94-ВР.
4. Про основні засади забезпечення кібербезпеки України: Закон України від 01.08.2022 № 2163-VIII.
5. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 01.07.2022 р. № 80/94-ВР.
6. Про державну таємницю: Закон України від 15.03.2022 №3855-XII.
7. Про доступ до публічної інформації: Закон України від 19.02.2022 № 2939-VI
8. Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 12.09.2009 р. № 505/98.
9. Про систему електронних підписів, що застосовується в межах Співтовариства: Директива 1999/93/ЄС Європейського парламенту та Ради від 13.12.99 р.
10. Про послуги на внутрішньому ринку: Директиви 2006/123/ЄС Європейського парламенту та Ради від 12 грудня 2006 року.
11. Про електронні ідентифікації та довірчі послуги для електронних транзакцій в межах внутрішнього ринка: Регламент (ЄС) №910/2014 Європейського парламенту та Ради Європи від 23/06/2014 року.
12. Про електронні документи та електронний документообіг: Закон України від 22.05.03 р. № 851-IV.
13. Про електронний цифровий підпис: Закон України від 22.05.03 р. № 852-IV.
14. Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII.
15. Про ліцензування господарської діяльності: Закон України від 21.03.2021 № 222-VIII.
16. Про Концепцію (основи державної політики) національної безпеки України: Постанова Верховної Ради України від 22.07.2003 № 3/97-ВР.
17. Про затвердження Концепції технічного захисту інформації в Україні: Постанова Кабінету Міністрів України від 13.10.2011 №1126-97-п.
18. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373.
19. Про затвердження переліку послуг у галузі технічного захисту інформації, господарська діяльність щодо надання яких підлягає ліцензуванню: Постанова Кабінету Міністрів України від 18.05.2011 року №517.
20. Про затвердження переліків послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та криптосистем і засобів криптографічного захисту інформації, господарська діяльність щодо яких підлягає ліцензуванню: Постанова Кабінету Міністрів України від 25.05.2011 року №543.
21. Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності: Постанова Кабінету Міністрів України від від 19 вересня 2018 р. № 749.
22. Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу: Постанова Кабінету Міністрів України від 26.05.04 р. № 680.
23. Про затвердження Положення про центральний засвідчувальний орган: Постанова Кабінету Міністрів України від 28.10.04 р. № 1451.
24. Про затвердження Порядку акредитації центру сертифікації ключів: Постанова Кабінету Міністрів України від 13.07.04 р. № 903.

25. Про затвердження Порядку обов’язкової передачі документованої інформації: Постанова Кабінету Міністрів України від 28.10.04 р. № 1454.

26. Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності : Постанова Кабінету Міністрів України від 28.10.04 р. № 1452.

27. Про затвердження Правил посиленої сертифікації: наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.01.05 р. № 3. – (Зареєстрований Міністерством юстиції України від 27.01.05 р. № 104/10384.

28. Про затвердження Правил проведення робіт із сертифікації засобів захисту інформації: наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України, Державного комітету України з питань технічного регулювання та споживчої політики від 25.04.007 р. № 75/91. – (Зареєстрований Міністерством юстиції України від 14.05.07 р. № 498/13765).

29. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації : наказ Державної служби спеціального зв’язку та захисту інформації України від 20.07.07 р. № 141. – (Зареєстрований Міністерством юстиції України від 30.07.07 р. № 862/14129).

30. Про затвердження Положення про державну експертизу у сфері криптографічного захисту інформації : наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 23.06.08 р. № 100. – (Зареєстрований Міністерством юстиції України від 16.07.2008 р. № 651/15342).

31. Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису : наказ Міністерства юстиції України та Державної служби спеціального зв’язку та захисту інформації України від 20.08.12 р. № 1236/5/453. – (Зареєстрований Міністерством юстиції України від 20.08.12 р. № 1398/21710).

32. Про затвердження Вимог до форматів криптографічних повідомлень: наказ Державної служби спеціального зв’язку та захисту інформації України від 18.12.12 р. № 739. – (Зареєстрований Міністерством юстиції України від 14.01.13 р. № 108/22640.

33. Про затвердження Регламенту роботи центрального засвідчувального органу: наказ Міністерства юстиції України від 29.01.13 р. № 183/5. – (Зареєстрований Міністерством юстиції України від 30.01.13 р. № 191/22723).

34. Щодо стану роботи з адаптації законодавства України до законодавства Європейського Союзу: Рішення шостого засідання Міжвідомчої координаційної ради з адаптації законодавства України до законодавства ЄС від 28.09.01 р.

35. Цивільний кодекс України від 16.01.2003 р. № 435-IV.

36. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» від 25 лютого 2017 року № 47/2017

37. Указ Президента України "Про деякі заходи з дерегулювання підприємницької діяльності" від 23.07.1998 № 817

38. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT)

39. ДСТУ 4145-2002. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. - К.: ДКУ з питань ТР СП, 2003. – 31с.

40. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

41. НД ТЗІ 1.1-003-99, «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу», - 30с.

42. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

43. Бабенко Т.В. Криптологія в тестах, задачах і прикладах: навч. посібник/ Т.В. Бабенко, Г.М. Гулак, С.О. Сушко, Л.Я. Фомічова. – Д.: Національний гірничий університет, 2013, - 318с.

44. Береза А. Електронна комерція: Навч. посібник / Київський національний економічний ун- т. — Київ.: КНЕУ, 2002. — 326с.

45. Богуш В.М. Криптографічні застосування елементарної теорії чисел: посібник / Богуш В.М., Мухачов В.А. - К.: вид. ДУІКТ, 2006. – 126с

46. Брижко В., Новицький А., Цимбалюк В., Швець М. Електронна комерція: правові заходи та заходи удосконалення: монографія / Науково-дослідний центр правової інформатики Академії правових наук України. — Київ.: НДЦПІ АПрНУ, 2008. — 149с.

47. Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія / Ю.І. Горбенко, І.Д. Горбенко; Харк. нац. ун-т радіоелектрон., ЗАТ Ін-т інформ. технологій. – Х.: Форт, 2010. – 593 с.

48. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування: монографія / І.Д. Горбенко, Ю.І. Горбенко; Харк. нац. ун-т радіоелектрон., ЗАТ «Ін-т інформ. Технологій». – Харків.: Форт, 2012. – 868 с.

49. Гулак Г.М. Основи криптографічного захисту інформації: підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук, Вінниц. нац. техн. ун-т.– Вінниця : ВНТУ, 2012.– 199 с.

50. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с.

51. Давидов М. В. Організація системи запровадження електронних підписів у електронному банківському бізнесі //Актуальні проблеми економіки. - 2004. - № 8. - С. 183 - 190.

52. Козіел Г. Електронний підпис - задачі і проблеми //Актуальні проблеми економіки. - 2005. - № 10. - С. 118 – 122

53. Локшин А. Особливості застосування електронного цифрового підпису //Секретарь-референт. - 2007. - № 12. - С. 23-24

54. Мельник Т. Електронний документообіг та електронний підпис //Бухгалтерський облік і аудит. - 2008. - № 7. - С. 47-53.

55. Мухачов В.А. Методи практичної криптографії: посібник / Мухачов В.А., Хорошко В.А. К.: ООО «ПоліграфКонсалтинг», 2005. – 215 с.

56. Петрицький А. Вчіться ставити електронний підпис //Злагода. - 2002. - № 3. - С. 15

57. Шпірко А. Запровадження та ефективне використання електронного документообігу й електронного підпису в Україні: проблеми, нові можливості, шляхи розвитку //Вісник Національного банку України. - 2005. - № 3. - С. 36-41.

58. Янчева Л. Електронна комерція: організація та облік: навч.посіб. / Харківський держ. ун-т харчування та торгівлі. — Харків. : ХДУХТ, 2008. — 231с.

59. ISO/IEC 8824, “Information technology-Abstract Syntax Notation One (ASN.1)“ specifies the structure and the notation of “Object Identifiers”

60. ISO/IEC 9594-8:2017 Information technology. Open Systems Interconnection. The Directory. Part 8: Public-key and attribute certificate frameworks.

61. RFC 2315. PKCS #7: Cryptographic Message Syntax Version 1.5 [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2315

62. RFC 2459. Internet X.509 Public Key Infrastructure: Certificate and CRL Profile [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2459

63. RFC 2510. Internet X.509 Public Key Infrastructure: Certificate Management Protocols [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2510

64. RFC 2511. Internet X.509 Certificate Request Message Format [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2511

65. RFC 2527. Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2527

66. RFC 2528. Internet X.509 Public Key Infrastructure: Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2528

67. RFC 2559. Internet X.509 Public Key Infrastructure: Operational Protocols - LDAPv2

[Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2559

68. RFC 2560. Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol – OCSP [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2560

69. RFC 2585. Internet X.509 Public Key Infrastructure: Operational Protocols: FTP and HTTP [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2585

70. RFC 2587. Internet X.509 Public Key Infrastructure: LDAPv2 Schema [Електронний ресурс]. – Режим доступу: https://www.ietf.org/rfc/rfc2587.txt

71. RFC 2797. Certificate Management Messages over CMS [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2797

72. RFC 2875. Diffie-Hellman Proof-of-Possession Algorithms [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2875

73. RFC 2985. PKCS #9: Selected Object Classes and Attribute Types Version 2.0 [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2985

74. RFC 2986. PKCS #10: Certification Request Syntax Specification Version 1.7 [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2986

75. RFC 3029. Internet X.509 Public Key Infrastructure: Data Validation and Certification Server Protocols [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc3029

76. RFC 3039. Internet X.509 Public Key Infrastructure: Qualified Certificates Profile [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc3039

77. RFC 3161. Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP) [Електронний ресурс]. – Режим доступу: https://www.ietf.org/rfc/rfc3161.txt

78. RFC 3279. Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc3279

79. RFC 3281. An Internet Attribute Certificate Profile for Authorization [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc3628

80. RFC 3282. Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc3280

81. RFC 3379. Delegated Path Validation and Delegated Path Discovery Protocol Requirements [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc3379

82. RFC 3628. Policy Requirements for Time-Stamping Authorities (TSAs) [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc3628

83. RFC 5208. Public-Key Cryptography Standards (PKCS) #8: Private-Key Information Syntax Specification Version 1.2 [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc5208

84. RFC 5280 Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile

85. RFC 5750 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling

86. RFC 6125 Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)

87. RFC 7292. PKCS #12: Personal Information Exchange Syntax v1.1 [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc7292

88. RFC 8017. PKCS #1: RSA Cryptography Specifications Version 2.2 [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc8017

89. RFC 8018. PKCS #5: Password-Based Cryptography Specification Version 2.0 [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2898

90. Burnett S., Paine S. RSA Security’s Official Guide to Cryptography / S. Burnett, S. Paine. - McGraw Hill Professional, 2001. 419 p.

91. Choudhury S. Public Key Infrastructure Implementation and Design / S. Choudhury, K. Bhatnagar, W. Haque. – New York: M&T Books, 2002. – 320 P.

92. Karamanian A. PKI Uncovered / A. Karamanian, S. Tenneti, F. Dessart. – Indianapolis,: Cisco Systems, Inc., 2011. – 270 P.

93. Stapleton J. J. A Guide to PKI Operations / J. J. Stapleton, W. Clay Epstein. – Boca Raton: Taylor & Francis Group, 2016. – 321 P.

Додаткова:

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К.: ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.

2. Єрмошин В.В., Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки. /Невойт Я.В., Єрмошин В.В.// Монографія. – К: ДУТ, 2015. – 124 С.

3. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. /В.Л. Бурячок, С.В. Толюпа, А.О. Аносов, В.А. Козачок, Н.В. Лукова-Чуйко/ –К.: ДУТ, 2015. – 345 с.

4. Богуш В.М., Юдін О.К., Інформаційна безпека держави. –К.: «МК-Прес», 2005. – 432с.

5. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.

6. Цимбалюк В.С. Інформаційне право (теорія і практика). Монографія. – К.: 2009. – 364с.

7. Кобозева А.А., Мачалін І.О., Хорошко В.О., Аналіз захищеності інформаційних систем. Підручник. – К.: вид. ДУІКТ, 2010. - 316 с.

8. Андрєєв В.І., Хорошко В.О., Чередніченко В.С., Шелест М.Є., Основи інформаційної безпеки. Підручник. – К.: вид. ДУІКТ, 2009. –292 с.

9. ISO/IEC 15408-1: Information technology. Security techniques - Evaluation criteria for IT security, Part 1: Introduction and general model, 1999.

10. ISO/IEC 15408-2: Information technology. Security techniques - Evaluation criteria for IT security, Part 2: Security functional requirements, 1999.

11. ISO/IEC 15408-3: Information technology. Security techniques - Evaluation criteria for IT security, Part 3: Security assuracce requirements, 1999. ISO/IEC 17799: Information technology - Code of practice for Information security management, 2000.

12. ISO/IEC 7498-2. Information processing systems Open Systems Interconnection Basic Reference Model. Part 2: Security Architecture. Switzeland, 1989. 32 pp.

13. Neumann P.G. Practical Architectures for survivable Systems and Networks. Technical Report. - SRI International: Computer Science Laboratory, 2001. - 209 pp. - http://www.csl.sri.com/neumann/survivability.dvi.

9. Додаткові інформаційні ресурси

1. Верховна Рада України. Законодавство України: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/

2. Державна служба спеціального зв’язку та захисту інформації: [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/index.

3. CERT-UA: [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/.