

**Інформаційний пакет освітніх компонент навчального плану
освітньо-професійної програми «Інформаційна та кібернетична безпека»**

(назва)

Освітнього рівня Бакалавр

Спеціальності 125 Кібербезпека

Галузь знань 12 Інформаційні технології

1. Назва освітньої компоненти Інфраструктура відкритих ключів

(назва дисципліни)

2. Тип вибіркова

3. Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
			5	150	18	0	36

4. Взаємозв'язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	<ul style="list-style-type: none"> 1. Прикладна криптологія 2. Основи захисту конфіденційних даних 3. Стандарти криптографічного захисту
Освітні компоненти для яких є базовою	<ul style="list-style-type: none"> 1. Комплексні системи захисту інформації 2. Кібербезпека банківських та комерційних структур

5. Компетенції відповідно до ОПШ та вимог роботодавців:

Компетенції відповідно до ООП

Знати	Вміти
1. Архітектуру, додатки та сервіси, що базуються на базі ІВК;	1. Розробляти політики ІВК, визначати необхідний перелік технологій та сервісів ІВК;
2. Нормативно-правову базу забезпечення ІВК;	2. Розробляти та визначати загальні принципи побудови ІВК, завдання, вихідні дані та фактори, які необхідно врахувати при проектуванні ІВК;
3. Порядок проектування та впровадження ІВК;	3. Здійснювати аналіз та оцінку параметрів ІВК;
4. Світові тенденції та рішення, щодо розгортання ІВК.	4. Здійснювати аналіз організаційної структури і взаємозв'язків

	елементів ІВК: 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 ІВК;
	5. Здійснювати аналіз та формування політики безпеки елементів ІВК: визначити основні складові політики безпеки, розробити систему документів, що забезпечують реалізацію політики безпеки, визначити гарантії правильності реалізації політики безпеки та її забезпечення;
	6. Здійснювати формування базових положень політики безпеки, розробити правила забезпечення інформаційної безпеки;
	7. Здійснювати оцінку ефективності систем захисту елементів ІВК;
	8. Застосовувати національні та міжнародні стандарти при аналізі та розробленні ІВК та (або) її елементів;
	9. Застосовувати типові підходи до проектування та налагодження сучасних ІВК, здійснити порівняння сучасних ІВК, здійснити порівняння підходів до організації типових інфраструктур;
	10. Оцінювати ефективність впровадження перспективних засобів та систем захисту інформаційних технологій, що використовується при створенні ІВК.
Компетенції відповідно до вимог роботодавців	
1. Законодавство України у галузі електронного цифрового підпису, електронного документообігу та захисту інформації;	1. Формувати базові положення політики безпеки, розробка правил забезпечення інформаційної безпеки;
2. Міжнародні стандарти електронного цифрового підпису та європейські стандарти ETSI серії Electronic Signatures and Infrastructures;	2. Формувати базові положення політики ІВК, визначити необхідний перелік технологій та сервісів ІВК;
3. Принципи побудови інфраструктури відкритих ключів, архітектури, додатків та сервісів, що базуються на базі ІВК;	3. Розробляти та визначити загальні принципи побудови ІВК, завдання, вихідні дані та фактори, які необхідно врахувати при проектуванні ІВК;
4. Світові тенденції та рішення, щодо впровадження ІВК.	4. Здійснювати аналіз організаційної структури і взаємозв'язків елементів ІВК;
	5. Проектувати системи ЕЦП (інфраструктури відкритих ключів) на базі продуктів Microsoft, «АВТОР», «ІТ» та інші;
	6. Розгортати та впроваджувати технології ІВК в інфраструктуру замовників.
6. Результати навчання відповідно до ОПІ	
1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.	

2. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
3. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
4. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і кібербезпеки.
5. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
6. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

7. План вивчення освітньої компоненти

Змістовний розділ	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка
Розділ 1						
	Лекція 1	Тема: Довіра в сфері електронних комунікацій	<ol style="list-style-type: none"> 1. світові тенденції та рішення, щодо розгортання ІВК; 2. архітектуру, додатки та сервіси, що базуються на базі ІВК; 3. нормативно-правову базу забезпечення ІВК. 	1. характеризувати ключові елементи та механізми довіри в сфері електронних комунікацій та електронної комерції.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87032
	Лекція 2	Тема: Основні компоненти та сервіси РКІ	<ol style="list-style-type: none"> 1. світові тенденції та рішення, щодо розгортання ІВК; 2. архітектуру, додатки та сервіси, що базуються на базі ІВК. 	<ol style="list-style-type: none"> 1. здійснювати аналіз та оцінку параметрів ІВК; 2. здійснювати аналіз організаційної структури і взаємозв'язків елементів ІВК. 	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87050
	Лекція 3	Тема: Моделі та механізми довіри	<ol style="list-style-type: none"> 1. архітектуру, додатки та сервіси, що базуються на базі ІВК. 	<ol style="list-style-type: none"> 1. здійснювати аналіз організаційної структури і взаємозв'язків елементів ІВК. 2. формувати опис інфраструктури та середовища її 	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87051

				функціонування; 3. здійснювати аналіз та формування політики безпеки елементів ІВК.	BY	
Лекція 4	Тема: Сертифікати відкритих ключів	1. архітектуру, додатки та сервіси, що базуються на базі ІВК; 2. світові тенденції та рішення, щодо розгортання ІВК.	1. застосовувати типові підходи до налагодження сучасних простих систем ІВК, здійснити порівняння сучасних ІВК.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87052	
Лекція 5	Тема: Класифікація сертифікатів та управління ними	1. архітектуру, додатки та сервіси, що базуються на базі ІВК; 2. світові тенденції та рішення, щодо розгортання ІВК; 3. нормативно-правову базу забезпечення ІВК.	1. аналізувати різновиди сертифікатів відкритих ключів.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87053	
Лекція 6	Тема: Політики, регламент і процедури РКІ	1. архітектуру, додатки та сервіси, що базуються на базі ІВК; 2. світові тенденції та рішення, щодо розгортання ІВК; 3. нормативно-правову базу забезпечення ІВК.	1. розробляти політики ІВК, визначати необхідний перелік технологій та сервісів ІВК; 2. здійснювати аналіз та формування політики безпеки елементів ІВК: визначити основні складові політики безпеки, розробити систему документів, що забезпечують реалізацію політики безпеки, визначити гарантії правильності реалізації політики безпеки та її	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87054	

				забезпечення; 3. здійснювати формування базових положень політики безпеки, розробити правила забезпечення інформаційної безпеки.		
Лекція 7	Тема: Стандарти і специфікації РКІ	1. архітектуру, додатки та сервіси, що базуються на базі ІВК; 2. світові тенденції та рішення, щодо розгортання ІВК; 3. нормативно-правову базу забезпечення ІВК.	1. застосовувати національні та міжнародні стандарти при аналізі та розробленні ІВК та (або) її елементів.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87055	
Лекція 8	Тема: Сервіси, що базуються на РКІ	1. архітектуру, додатки та сервіси, що базуються на базі ІВК; 2. світові тенденції та рішення, щодо розгортання ІВК.	1. здійснювати аналіз основних сервісів, що базуються на ІВК; 2. здійснити аналіз основних криптографічних механізмів.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87056	
Практичне заняття 1	Тема: Механізми аутентифікації	1. світові тенденції та рішення, щодо розгортання ІВК; 2. архітектуру, додатки та сервіси, що базуються на базі ІВК.	1. характеризувати ключові елементи та механізми довіри в сфері електронних комунікацій та електронної комерції.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87033	
Практичне заняття 2	Тема: Основні компоненти і сервіси РКІ	1. світові тенденції та рішення, щодо розгортання ІВК; 2. архітектуру, додатки та сервіси, що базуються на базі ІВК.	1. здійснювати аналіз та оцінку параметрів ІВК; 2. здійснювати аналіз організаційної структури і взаємозв'язків елементів ІВК.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87061	

					=f8gFElipBY	
Практичне заняття 3	Тема: Сервіси безпеки РКІ та базові криптографічні механізми	1. світові тенденції та рішення, щодо розгортання ІВК; 2. архітектуру, додатки та сервіси, що базуються на базі ІВК.	1. здійснювати аналіз та оцінку параметрів ІВК; 2. характеризувати ключові елементи та механізми довіри в сфері електронних комунікацій та електронної комерції..		http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87062
Практичне заняття 4	Тема: Класифікація сертифікатів і керування ними	1. світові тенденції та рішення, щодо розгортання ІВК; 2. нормативно-правову базу забезпечення ІВК.	1. аналізувати різновиди сертифікатів відкритих ключів.		http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87063
Практичне заняття 5	Тема: Формат списків анульованих сертифікатів	1. світові тенденції та рішення, щодо розгортання ІВК; 2. нормативно-правову базу забезпечення ІВК.	1. застосовувати національні та міжнародні стандарти при аналізі та розробленні ІВК та (або) її елементів.		http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87064
Практичне заняття 6	Тема: Типи списків анульованих сертифікатів і схеми анулювання	1. світові тенденції та рішення, щодо розгортання ІВК; 2. нормативно-правову базу забезпечення ІВК.	1. застосовувати типові підходи до формування списків анульованих сертифікатів, схеми анулювання та їх розповсюдження		http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87065
Практичне заняття 7	Тема: Основні типи архітектури РКІ	1. світові тенденції та рішення, щодо розгортання	1. здійснювати аналіз та оцінку параметрів ІВК;		http://dl.dut.edu.ua/	http://dl.dut.edu.ua/mod/re

			ІВК; 2. архітектуру, додатки та сервіси, що базуються на базі ІВК.	2. здійснювати аналіз організаційної структури і взаємозв'язків елементів ІВК.	course/view.php?id=624&edit=0&sesskey=f8gFElipBY	source/view.php?id=87066
Практичне заняття 8	Тема: Валідація шляху сертифікації		1. світові тенденції та рішення, щодо розгортання ІВК; 2. архітектуру, додатки та сервіси, що базуються на базі ІВК.	1. здійснювати аналіз та оцінку параметрів ІВК; 2. здійснювати аналіз організаційної структури і взаємозв'язків елементів ІВК.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87067
Практичне заняття 9	Тема: Механізми розповсюдження інформації РКІ		1. світові тенденції та рішення, щодо розгортання ІВК; 2. архітектуру, додатки та сервіси, що базуються на базі ІВК.	1. здійснювати аналіз організаційної структури і взаємозв'язків елементів ІВК.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87068
Практичне заняття 10	Тема: Опис політики РКІ		1. світові тенденції та рішення, щодо розгортання ІВК; 2. архітектуру, додатки та сервіси, що базуються на базі ІВК; 3. нормативно-правову базу забезпечення ІВК.	1. розробляти політики ІВК, визначати необхідний перелік технологій та сервісів ІВК; 2. здійснювати аналіз та формування політики безпеки елементів ІВК: визначити основні складові політики безпеки, розробити систему документів, що забезпечують реалізацію політики безпеки, визначити гарантії	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87069

				правильності реалізації політики безпеки та її забезпечення; 3. здійснювати формування базових положень політики безпеки, розробити правила забезпечення інформаційної безпеки.		
Практичне заняття 11	Тема: Сервіси, що базуються на РКІ	1. світові тенденції та рішення, щодо розгортання ІВК.	1. здійснювати аналіз основних сервісів, що базуються на ІВК; 2. здійснити аналіз основних криптографічних механізмів.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87070	
Практичне заняття 12	Тема: Додатки, що базуються на РКІ	1. світові тенденції та рішення, щодо розгортання ІВК.	1. здійснювати аналіз типових додатків ІВК; 2. здійснити аналіз потрібних технологій обробки інформації, аналіз складу та характеристик елементів ІВК.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87071	
Самостійна робота	Тема 1: Механізми аутентифікації Тема 2: Основні компоненти і сервіси РКІ Тема 3: Сервіси безпеки РКІ та базові криптографічні механізми Тема 4: Класифікація сертифікатів і керування ними Тема 5: Формат списків	1. світові тенденції та рішення, щодо розгортання ІВК; 2. архітектуру, додатки та сервіси, що базуються на базі ІВК; 3. нормативно-правову базу забезпечення ІВК.	1. характеризувати ключові елементи та механізми довіри в сфері електронних комунікацій та електронної комерції; 2. здійснювати аналіз та оцінку різноманітних механізмів аутентифікації; 3. здійснювати аналіз та оцінку параметрів ІВК; 4. здійснювати аналіз організаційної структури і	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87029	

		<p>анульованих сертифікатів Тема 6: Типи списків анульованих сертифікатів і схеми анулювання Тема 7: Основні типи архітектури PKI Тема 8: Валідація шляху сертифікації Тема 9: Механізми розповсюдження інформації PKI Тема 10: Опис політики PKI Тема 11: Сервіси, що базуються на PKI Тема 12: Додатки, що базуються на PKI</p>		<p>взаємозв'язків елементів ІВК; 5. формувати опис інфраструктури та середовища її функціонування; 6. здійснювати аналіз та формування політики безпеки елементів ІВК; 7. застосовувати типові підходи до налагодження сучасних простих систем ІВК, здійснити порівняння сучасних ІВК; 8. аналізувати різновиди сертифікатів відкритих ключів; 9. розробляти політики ІВК, визначати необхідний перелік технологій та сервісів ІВК; 10. здійснювати аналіз та формування політики безпеки елементів ІВК: визначити основні складові політики безпеки, розробити систему документів, що забезпечують реалізацію політики безпеки, визначити гарантії правильності реалізації політики безпеки та її забезпечення; 11. здійснювати формування базових</p>		
--	--	--	--	--	--	--

				<p>положень політики безпеки, розробити правила забезпечення інформаційної безпеки;</p> <p>12. застосовувати національні та міжнародні стандарти при аналізі та розробленні ІВК та (або) її елементів.</p> <p>13. здійснювати аналіз основних сервісів, що базуються на ІВК;</p> <p>14. здійснити аналіз основних криптографічних механізмів;</p> <p>15. здійснювати аналіз типових додатків ІВК;</p> <p>16. здійснити аналіз потрібних технологій обробки інформації, аналіз складу та характеристик елементів ІВК.</p>		
Розділ 2						
	Лекція 9	Підготовка до розгортання РКІ	1. порядок проектування та впровадження ІВК.	<p>1. здійснити аналіз потрібних технологій обробки інформації, аналіз складу та характеристик елементів ІВК;</p> <p>2. здійснювати аналіз організаційної структури і взаємозв'язків елементів ІВК: формувати опис інфраструктури та середовища її функціонування, визначити склад</p>	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87057

				потрібного апаратного та програмного забезпечення.		
	Лекція 10	Проблеми вибору постачальника технології або сервісів РКІ	1. порядок проектування та впровадження ІВК; 2. світові тенденції та рішення, щодо розгортання ІВК.	1. здійснити порівняння сучасних ІВК; 2. здійснити порівняння підходів до організації типових інфраструктур; 3. здійснювати оцінку ефективності систем захисту елементів ІВК.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87058
	Лекція 11	Проектування і впровадження РКІ	1. порядок проектування та впровадження ІВК; 2. світові тенденції та рішення, щодо розгортання ІВК.	1. застосовувати національні та міжнародні стандарти при аналізі та розробленні ІВК та (або) її елементів; 2. застосовувати типові підходи до проектування та налагодження сучасних ІВК.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87059
	Лекція 12	Проблеми реалізації РКІ	1. порядок проектування та впровадження ІВК; 2. світові тенденції та рішення, щодо розгортання ІВК.	1. оцінювати ефективність впровадження перспективних засобів та систем захисту інформаційних технологій, що використовується при створенні ІВК.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87060
	Практичне заняття 13	Підготовка до розгортання РКІ	1. порядок проектування та впровадження ІВК.	1. здійснити аналіз потрібних технологій обробки інформації, аналіз складу та характеристик елементів ІВК; 2. здійснювати аналіз організаційної структури і взаємозв'язків елементів ІВК: формувати опис	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87074

				інфраструктури та середовища її функціонування, визначити склад потрібного апаратного та програмного забезпечення.		
	Практичне заняття 14	Вибір технології або сервісів РКІ	1. порядок проектування та впровадження ІВК; 2. світові тенденції та рішення, щодо розгортання ІВК.	1. здійснити порівняння сучасних ІВК; 2. здійснити порівняння підходів до організації типових інфраструктур; 3. здійснювати оцінку ефективності систем захисту елементів ІВК.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87075
	Практичне заняття 15	Проектування та впровадження РКІ	1. порядок проектування та впровадження ІВК; 2. світові тенденції та рішення, щодо розгортання ІВК.	1. застосовувати національні та міжнародні стандарти при аналізі та розробленні ІВК та (або) її елементів; 2. застосовувати типові підходи до проектування та налагодження сучасних ІВК.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87077
	Практичне заняття 16	Проектування та розгортання РКІ на базі Microsoft SA	1. порядок проектування та впровадження ІВК.	1. застосовувати національні та міжнародні стандарти при аналізі та розробленні ІВК та (або) її елементів; 2. застосовувати типові підходи до проектування та налагодження сучасних ІВК.	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87078
	Практичне заняття 17	Проблеми реалізації РКІ	1. порядок проектування та впровадження ІВК; 2. світові тенденції та рішення, щодо розгортання	1. оцінювати ефективність впровадження перспективних засобів та систем захисту	http://dl.dut.edu.ua/course/view.php?id=	http://dl.dut.edu.ua/mod/resource/view.php?id=87076

			ІВК.	інформаційних технологій, що використовується при створенні ІВК.	624&edit=0&sesskey=f8gFElipBY	
	Самостійна робота	Тема 13: Підготовка до розгортання РКІ Тема 14: Вибір технології або сервісів РКІ Тема 15: Проектування та впровадження РКІ Тема 16: Проектування та розгортання РКІ на базі Microsoft SA Тема 17: Проблеми реалізації РКІ	1. порядок проектування та впровадження ІВК; 2. світові тенденції та рішення, щодо розгортання ІВК.	1. здійснити аналіз потрібних технологій обробки інформації, аналіз складу та характеристик елементів ІВК; 2. здійснювати аналіз організаційної структури і взаємозв'язків елементів ІВК: формувати опис інфраструктури та середовища її функціонування, визначити склад потрібного апаратного та програмного забезпечення; 3. здійснити порівняння сучасних ІВК; 4. здійснити порівняння підходів до організації типових інфраструктур; 5. здійснювати оцінку ефективності систем захисту елементів ІВК; 6. застосовувати національні та міжнародні стандарти при аналізі та розробленні ІВК та (або) її елементів; 7. застосовувати типові підходи до проектування та налагодження сучасних ІВК;	http://dl.dut.edu.ua/course/view.php?id=624&edit=0&sesskey=f8gFElipBY	http://dl.dut.edu.ua/mod/resource/view.php?id=87029

				8. оцінювати ефективність впровадження перспективних засобів та систем захисту інформаційних технологій, що використовується при створенні ІВК		
8. Мова вивчення освітньої компоненти						
Українська						
Англійська: Додатки, що базуються на РКІ; Проектування та впровадження РКІ.						
9. Інформаційне забезпечення освітньої компоненти						
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, 2011.– 198 с.						
Stapleton J.J. Security without Obscurity A guide to PKI Operations / J.J. Stapleton, W. Clay Epstein. NW: Taylor & Francis Group, 2016.- 321 p.						
Ristić I. OpenSSL Cookbook / Ivan Ristić. Feisty Duck – Fine technology book. March 2016.						
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”.– Х. : Форт, 2012. – 868 с.						
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.						
10. Методи оцінювання, підсумкові звітності за освітньою компонентою						
Екзамен						
11. Матеріально-технічне забезпечення освітньої компоненти						
Комп’ютерні лабораторії кафедри ІКБ: 419, 421						
Програмно-апаратне забезпечення: Certificate Authority на базі Windows 2016 (Microsoft Certificate Services), ПТК ЦСК «CryptoKDC» (АВТОР), ПТК ЦСК «ІТ», PGPDesktop (Symantec), OpenSSL.						