

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Інститут комп'ютерних наук та інформаційних технологій
/назва навчально-наукового інституту/

Кафедра інформаційних систем та мереж
/назва /

«ЗАТВЕРДЖУЮ»

Голова науково-методичної комісії
спеціальності «Інформаційні системи і
технології»

 /Гайчишук В.В. /
/підпис/ /ініціали та прізвище /
« 30 » 08 20 19 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

В-11 «Безпека розподілених інформаційних систем»

/код і назва навчальної дисципліни/

Другий (магістерський)

/рівень вищої освіти/

галузь знань **12 Інформаційні технології**

/шифр і назва/

спеціальність **126 «Інформаційні системи і технології»**

/шифр і назва /

вид дисципліни **вибіркова**

(обов'язкова / за вибором)

мова викладання **українська**

Львів – 2019 рік

Робоча програма з навчальної дисципліни «Безпека розподілених інформаційних систем» для студентів Інституту комп'ютерних наук та інформаційних технологій
/назва інституту/

Розробник:

Доц., к.т.н., доц. _____
/посада, науковий ступінь та вчене звання/

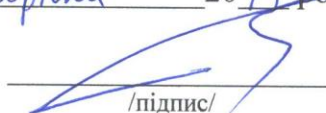

/підпис/

/ П.О. Кравець /
/ініціали та прізвище/

Робоча програма розглянута та схвалена на засіданні кафедри ІСМ

Протокол від «28» серпня 2019 року № 1

Завідувач кафедри ІСМ


/підпис/

/ В.В.Литвин /
/ініціали та прізвище /

Робоча програма розглянута та схвалена НМК спеціальності 126 "Інформаційні системи і технології"

Протокол від «26» 08 2019 року № 1

Секретар НМК


/підпис/

/ Т.В.Шестакова /
/ініціали та прізвище /

1. Структура навчальної дисципліни

Найменування показників	Всього годин	
	Денна форма навчання	Заочна форма навчання
Кількість кредитів/год.	4/120	—
Усього годин аудиторної роботи, у т.ч.:	45	—
• лекційні заняття, год.	15	—
• семінарські заняття, год.	—	—
• практичні заняття, год.	—	—
• лабораторні заняття, год.	30	—
Усього годин самостійної роботи, у т.ч.:	75	—
• контрольні роботи, к-сть/год.	—	—
• розрахункові (розрахунково-графічні) роботи, к-сть/год.	1/24	—
• індивідуальне науково-дослідне завдання, к-сть/год.	—	—
• підготовка до навчальних занять та контрольних заходів, год.	51	—
Екзамен	+	—
Залік	—	—

Частка аудиторного навчального часу студента у відсотковому вимірі:

- денної форми навчання – 37,5%;
- заочної форми навчання – —

2. Мета та завдання навчальної дисципліни

2.1. Мета вивчення навчальної дисципліни

Забезпечити студентам здобуття поглиблених теоретичних знань, практичних навичок, та умінь у галузі інформаційної безпеки розподілених систем для успішного виконання ними професійних обов'язків за спеціальністю «Інформаційні системи і технології» (ІСТ), спеціалізація «Розподілені інформаційні системи».

2.2. Завдання навчальної дисципліни

Внаслідок вивчення навчальної дисципліни студент повинен бути здатним продемонструвати такі **результати навчання**:

- 1) Здатність використовувати поглиблені теоретичні та фундаментальні знання, уміння і навички з безпеки розподілених інформаційних систем для успішного розв'язування складних спеціалізованих задач та практичних проблем під час професійної діяльності у галузі інформаційних систем та технологій або у процесі навчання, що передбачає застосування теорій та методів відповідної навчальної дисципліни і характеризується комплексністю та невизначеністю умов.
- 2). Володіння знаннями і розуміння наукових засад безпеки розподілених інформаційних систем.
- 3). Здатність формувати теоретичні та практичні рішення для проектування та супроводження систем захисту інформації.

- 4). Здатність застосувати знання та практичні навички аналізу відповідних нормативних документів, чинних стандартів і технічних умов у галузі.
- 5). Практичне застосування знань сучасного стану справ та новітніх технологій в галузі безпеки розподілених інформаційних систем.

Вивчення навчальної дисципліни передбачає формування та розвиток у студентів компетентностей:

загальних:

- 1). Здатність до абстрактного мислення, аналізу та синтезу на відповідних рівнях.
- 2). Здатність застосовувати знання у практичних ситуаціях.
- 3). Знання та розуміння предметної області та професійної діяльності.
- 4). Здатність спілкуватися, читати та писати іноземною мовою.
- 5). Навички використання інформаційних і комунікаційних технологій.
- 6). Здатність вчитися і оволодівати сучасними знаннями.
- 7). Здатність до пошуку, оброблення та узагальнення інформації з різних джерел.
- 8). Здатність працювати в команді та особисто.
- 9). Навички міжособистісної взаємодії.
- 10). Здатність розробляти та управляти проектами.
- 11). Навички здійснення безпечної діяльності.
- 12). Здатність оцінювати та забезпечувати якість виконуваних робіт.
- 13). Здатність діяти соціально відповідально та свідомо.

фахових:

- 1). Здатність проводити аналіз об'єкту проектування та предметної області.
- 2). Володіння навчально-методичними основами і стандартами в області ІСТ, уміння їх застосовувати при розробці функціональних профілів ІСТ, при побудові та інтеграції систем, продуктів і сервісів ІСТ.
- 3). Здатність до проектування системного, комунікаційного і прикладного програмного забезпечення, технічних засобів та комунікаційних й інформаційних технологій, мереж та систем.
- 4). Здатність розробляти засоби реалізації ІСТ (методичні, інформаційні, алгоритмічні, технічні й програмні).
- 5). Здатність розробляти, налагоджувати та вдосконалювати програмне забезпечення комп'ютерно-інтегрованих систем.
- 6). Здатність використовувати сучасні технології проектування в розробці алгоритмічного та програмного забезпечення ІСТ.
- 7). Здатність застосовувати, впроваджувати та експлуатувати сучасні ІСТ (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних) у різних галузях людської діяльності, національної економіки та виробництва.
- 8). Здатність до участі у роботах з доведення й освоєння ІСТ у ході впровадження, експлуатації та підготовки документації з менеджменту якості ІСТ.
- 9). Здатність управляти якістю продуктів і сервісів ІСТ протягом їх життєвого циклу.
- 10). Здатність проводити оцінку виробничих і невиробничих витрат на забезпечення якості об'єкта проектування, розробляти бізнес-рішення та оцінювати нові технологічні пропозиції.
- 11). Вибирати, проектувати, розгортати, інтегрувати, управляти, адмініструвати та супроводжувати застосування комунікаційних мереж, сервісів та інфраструктури організації.

- 12). Здатність здійснювати організацію робочих місць, їх технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів організаційно-управлінської діяльності.
- 13). Здатність формулювати та коректно ставити завдання та керувати молодшим технічним персоналом; пов'язувати технічні та управлінські підрозділи організації, а також брати активну участь у навчанні користувачів.
- 14). Здатність розуміти, розгортати, організовувати, управляти та користуватися сучасними навчально-дослідницькими ІСТ (у тому числі такими, що базуються на використанні Інтернету), інформаційними та комунікаційними технологіями.
- 15). Здатність проводити обчислювальні експерименти, зіставляти результати експериментальних даних і отриманих рішень та оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів, статей і доповідей на науково-технічних конференціях.
- 16). Здатність формувати нові конкурентоспроможні ідеї й реалізовувати їх у проектах (стартапах).
- 17). Здатність формулювати (роблячи презентації, або представляючи звіти) нові гіпотези та наукові задачі в області інформаційних технологій та розподілених систем баз даних та знань.
- 18). Здатність ефективно вибирати належні напрями і відповідні методи для розв'язування задач в області інформаційних технологій та розподілених систем баз даних та знань.
- 19). Здатність ефективно здійснювати вибір концептуальної моделі середовища розподілених систем баз даних та знань на основі структурного та об'єктно-орієнтованого підходів,
- 20). Здатність ефективно здійснювати параметризацію компонентів середовища розподілених систем баз даних та знань, формувати вимоги відповідності таких систем технічному завданню.

Результати навчання даної дисципліни деталізують такі **програмні результати навчання:**

- 1). Здатність використовувати поглиблені професійно-профільні знання та практичні навичками для оптимізації проектування інформаційних систем будь-якої складності, для вирішення конкретних завдань проектування інтелектуальних інформаційних систем з управління об'єктами різної фізичної природи.
- 2). Здатність формулювати та вдосконалювати важливу дослідницьку задачу, для її вирішення збирати необхідну інформацію та формулювати висновки, які можна захищати в науковому контексті.
- 3). Здатність проводити системний аналіз об'єктів проектування та обґрунтовувати вибір структури, алгоритмів та способів опрацювання інформації в ІСТ.
- 4). Здатність аргументувати вибір програмних та технічних засобів для створення ІСТ на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів ІСТ.
- 5). Здатність демонструвати знання сучасного рівня та новітніх технологій ІСТ з метою їх запровадження у професійної діяльності.
- 6). Здатність брати участь у проектуванні ІСТ, мати базові знання зі змісту і правил оформлення проектних матеріалів, знати склад та послідовність виконання проектних робіт з урахуванням вимог відповідних нормативно-правових документів.
- 7). Вміти обґрунтовувати вибір технічної структури та розробляти відповідне програмне забезпечення, що входить до складу ІСТ.
- 8). Здатність демонструвати знання і практичні навички програмування та використання прикладних і спеціалізованих комп'ютерних систем та середовищ для розв'язання задач проектування.

- 9). Здатність розуміти і враховувати соціальні, екологічні, етичні, економічні аспекти, вимоги охорони праці, виробничої санітарії, пожежної безпеки та наявних державних і закордонних стандартів під час формування технічних завдань та рішень.
- 10). Здатність демонструвати вміння розробляти техніко-економічне обґрунтування розроблення ІСТ та вміння оцінювати економічну ефективність їх впровадження.
- 11). Уміння спілкуватись англійською мовою в обсязі, достатньому для здійснення професійної діяльності, читання та трактування міжнародних технічних стандартів.
- 12). Здатність до аналізу предметної області та синтезу інформаційних систем та технологій із використанням сучасних методів та засобів інформаційних технологій.
- 13). Вміння застосовувати методи пошуку джерел інформації; аналізувати якість отриманої інформації.
- 14). Вміння застосовувати знання і розуміння для ідентифікації, формулювання і вирішення технічних задач спеціальності, використовуючи відомі методи.
- 15). Здатність використовувати технології моделювання; подання моделі в математичному і алгоритмічному вигляді; оцінювати якість моделі.
- 16). Вміння моделювати процеси в інформаційних системах і мережах; проводити аналіз об'єктів впровадження інформаційних технологій і особливостей їх використання в прикладних областях.
- 17). Системно мислити та застосовувати творчі здібності до формування принципово нових ідей; формувати, аналізувати і приймати рішення про найбільш перспективні проектні рішення.
- 18). Здатність працювати з експертними та текстологічними джерелами інформації для інтеграції даних і знань в області діяльності організації за допомогою методів набуття знань, подання знань, класифікації і компіляції знань; проектувати та використовувати наявні засоби інтеграції даних, опрацьовувати дані, що зберігаються у різних системах.
- 19). Здатність розробляти математичні моделі і алгоритми функціонування розподілених систем баз даних та знань розпізнавання образів і класифікації об'єктів в інтелектуальних інформаційних системах в умовах проектування систем розпізнавання образів за допомогою відповідного математичного забезпечення, використовуючи процедури формального уявлення про систему.
- 20). Здатність розробляти бази знань в умовах проектування інтелектуальних систем за допомогою відповідного програмного забезпечення, використовуючи результати обстеження, запити, особливості обраного способу подання знань.
- 21). Здатність будувати моделі інформаційних потоків, проектувати сховища і простори даних, бази знань, використовуючи діаграмну техніку і стандарти розроблення інформаційних систем.
- 22). Здатність створювати математичні моделі і алгоритми прийняття рішень за допомогою алгоритмічного та програмного забезпечення, використовуючи машинне навчання, штучні нейронні мережі, еволюційне моделювання, генетичні методи оптимізації, метод індуктивного моделювання та математичний апарат нечіткої логіки.
- 23). Уміння спілкуватись, включаючи усну та письмову комунікацію українською та іноземною мовами (англійською, німецькою, італійською, французькою, іспанською).
- 24). Здатність використання різноманітних методів, зокрема сучасних інформаційних технологій, для ефективного спілкування на професійному та соціальному рівнях.
- 25). Здатність адаптуватись до нових ситуацій та приймати відповідні рішення.
- 26). Здатність усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань.
- 27). Здатність відповідально ставитись до виконуваної роботи, самостійно приймати рішення, досягати поставленої мети з дотриманням вимог професійної етики.
- 28). Здатність демонструвати розуміння основних екологічних засад, охорони праці та безпеки життєдіяльності та їх застосування.

2.3. Перелік попередніх та супутніх і наступних навчальних дисциплін

№ з/п	Попередні навчальні дисципліни	Супутні і наступні навчальні дисципліни
1.	Інженерія даних і знань	Інформаційні технології комп'ютерних мереж
2	Методи опрацювання великих даних	Технології проектування систем бізнес-аналітики
3	Інформаційний маркетинг та менеджмент	Нереляційні бази даних

3. Анотація навчальної дисципліни

Знання отримані в процесі вивчення даної дисципліни базуються на ключових положеннях інформатики, інформаційних технологій, технологіях комп'ютерного проектування, сучасних методах та інструментах безпеки і управління розподіленими системами.

4. Опис навчальної дисципліни

4.1. Лекційні заняття

№ з/п	Назви тем	Кількість годин	
		ДФН	ЗФН
1	Архітектура та складові частини систем захисту інформації. Об'єкти захисту розподілених інформаційних систем. Основні джерела небезпек для розподілених інформаційних систем. Міжнародні та корпоративні стандарти захисту розподілених інформаційних систем	2	—
2	Методи та засоби інформаційної безпеки в розподілених інформаційних системах.	2	—
3	Криптографічні методи захисту інформації. Сучасні симетричні криптосистеми	2	—
4	Криптографічні методи захисту інформації. Асиметричні криптосистеми	2	—
5	Аутентифікація та ідентифікація об'єктів та суб'єктів розподіленої інформаційної системи. Електронний цифровий підпис.	2	—
6	Мережа та безпека інформації. Вплив типу та архітектури мережі на безпеку інформації. Огляд безпеки протоколів обміну даними	2	—
7	Безпека каналів передачі даних. Віртуальні мережі. Мережні екрани	2	—
8	Безпека комерційних операцій в Internet	1	—
Усього годин		15	—

4.2. Лабораторні заняття

№ з/п	Назви тем	Кількість годин	
		ДФН	ЗФН
1.	Шифр Віженера.	2	—
2.	Шифр одноразового блокноту.	4	—
3.	Шифрування DES.	4	—
4.	Афінний шифр заміни.	4	—
5.	Криптосистема RSA з відкритим ключем.	4	—
6.	Криптосистема Рабіна з відкритим ключем.	4	—
7.	Імовірнісна криптосистема Ель-Гамала з відкритим ключем.	4	—
8.	Алгоритм цифрового підпису DSA.	4	—
Усього годин		30	—

4.3. Самостійна робота

№ п/п	Зміст роботи	ДФН	ЗФН
1	Підготовка до лабораторних робіт	26	—
2	Підготовка до лекційних занять	15	—
3	Підготовка до екзаменаційного контролю	10	—
4	Виконання розрахункової роботи	24	—
Всього:		75	—

5. Методи діагностики знань

Діагностика знань відбувається шляхом оцінювання виконаних лабораторних робіт та екзаменаційного контролю (письмової компоненти) у формі тестових запитань трьох рівнів складності.

6. Критерії оцінювання результатів навчання студентів

Розподіл балів у 100-бальній шкалі	
Виконання лабораторних робіт	30 балів
Виконання розрахункової роботи	10 балів
Екзаменаційний контроль	60 балів
Разом за дисципліну	100 балів

7. Навчально-методичне забезпечення

Конспект лекцій, методичні вказівки до виконання лабораторних робіт, методичні вказівки для забезпечення самостійної роботи.

8. Рекомендована література

Базова

1. Мельников В.В. Защита информации в компьютерных системах / В.В. Мельников. – М.: Финансы и статистика, 1997. – 386 с.
2. Стенг Д. Секреты безопасности сетей / Д. Стенг, С. Мун. – К.: Диалектика, 1995. – 544 с.

3. Мафтик С. Механизмы защиты в сетях ЭВМ / С. Мафтик. – М.: Мир, 1993.
4. Организация и современные методы защиты информации // Под ред. Диева С.А., Шавасва А.Г. – М.: Концерн „Банковский деловой центр”, 1998. – 472 с.
5. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В двух книгах / В.А. Герасименко. – М.: Энергоатомиздат, 1994. – 576 с.
6. Девянин П.Н. Теоретические основы компьютерной безопасности. Уч. Пособие для ВУЗов / П.Н. Девянин. – М.: Радио и связь, 2002.
7. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В.Ф. Шаньгин. М.: Радио и связь, 1999.
8. Ухлинов А. М. Управление безопасностью информации в автоматизированных системах / А.М. Ухлинов. М.: МИФИ, 1996.
9. Смит Р. Аутентификация: от паролей до открытых ключей / Р. Смит. – М.: Вильямс, 2002. – 432 с.
10. Ховард М. Разработка защищенных Web-приложений на платформе Microsoft Windows 2000 / М. Ховард, М. Леви, Р. Вэймир. — СПб.: Питер; М: Русская Редакция, 2001. – 464 с.
11. Вербицкий О.В. Вступ до криптології / О.В. Вербицкий. – Львів: ВНТЛ, 1998. – 247 с.
12. Столлингс В. Криптография и защита сетей: принципы и практика / В. Столлингс. – 2-е изд. – М.: Вильямс, 2001. – 672 с.
13. Молдовян А. А. Криптография / А.А. Молдовян, Н.А. Молдовян, Б.Я. Советов. СПб.: «Лань», 2000.
14. Конхейм А. Г. Основы криптографии / А.Г. Конхейм. М.: Радио и связь, 1987.
15. Венбо М. Современная криптография. Теория и практика = Modern Cryptography: Theory and Practice / Мао Венбо. – М.: Вильямс, 2005. – 768 с.
16. Нечаев В.И. Элементы криптографии (Основы теории защиты информации) / В.И. Нечаев. – М.: Высшая школа, 1999.
17. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.

Допоміжна

1. Баричев С.Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М.: Горячая линия. – Телеком, 2002. – 175 с.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Триумф, 2002. – 816 с.
3. Щербаков А.Ю. Прикладная криптография: использование и синтез криптографических интерфейсов / А.Ю. Щербаков, А.В. Домашев. – М.: Русская Редакция, 2003. – 416 с.
4. Масленников М. Практическая криптография / М. Масленников. – СПб.: БХВ-Петербург, 2003. – 464 с.
5. Бернет С. Криптография. Официальное руководство RSA Security / С. Бернет, С. Пэйн. – М.: Бином-Пресс, 2002 г. – 384 с.
6. Рябко Б.Я. Основы современной криптографии для специалистов в информационных технологиях / Б.Я. Рябко, А.Н. Фионов. – М.: Научный мир, 2004.
7. Фергюсон Н. Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems / Нильс Фергюсон, Брюс Шнайер. – М.: «Диалектика», 2004. — 432 с.
8. Жежнич П.І. Технології інформаційного менеджменту: навч. посіб. / П.І. Жежнич. – Л. : Вид-во Львів. політехніки, 2010. – 260 с.
9. Палеха Ю.І. Інформаційний бізнес : підручник / Ю.І. Палеха, Ю.І. Горбань — К.: Вид-во Ліра-К. 2015.- 492 с.
10. Пістунов І.М. Інформаційний менеджмент: Матеріали метод. забезп. Дисципліни / І.М. Пістунов, Т.В. Борщ. – Д.: Національний гірничий університет, 2007. – 87 с.
11. Єжова Л.Ф. Інформаційний маркетинг: Навч.-метод. посіб. для самост. Вивч / Л.Ф.

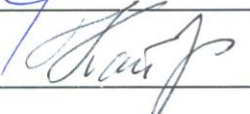
Єжова. – К.: КНЕУ, 2004. – 185 с.

12. Вовчак І.С. Інформаційні системи та комп'ютерна техніка в менеджменті: Навч. Посіб / І.С. Вовчак. – Тернопіль: Карт-бланш, 2002. – 354 с.

9. Інформаційні ресурси

1. Лазарева С.Ф. Економіка та організація інформаційного бізнесу / С.Ф. Лазарева. – Навчальний посібник. – [Електронний ресурс] / Режим доступу : <http://uchebnik-online.net/book/588-ekonomika-ta-organizaciya-informacijnogo-biznesu-navchalnij-posibnik-lazaryeva-s-f/1-soderzhanie.html>
2. Криптографія: загальні визначення, класифікація. Асиметричні та симетричні криптоалгоритми, їх порівняння. – <https://mozolevska09.wordpress.com/2014/03/14/криптографія-загальні-визначення-кл/>.
3. Основи функціонування систем криптографічного захисту інформації. – <http://buklib.net/books/28747/>.
4. Квантовая криптография. Учебное пособие / Д.А. Кронберг, Ю.И. Ожигов, А.Ю. Чернявский. – http://sqi.cs.msu.su/store/storage/ss8dw5n_quantum_cryptography.pdf.
5. ISO [Електронний ресурс] // Офіційний сайт ISO. – Режим доступу: <http://www.iso.org/iso/home.htm>.

10. Узгодження з іншими навчальними дисциплінами

№ з/п	Назва навчальної дисципліни, щодо якої проводиться узгодження	Прізвище та ініціали викладача	Підпис
1.	Технології підтримки процесів прийняття рішень	Верес О.М.	
2.	Методи прийняття рішень в активних середовищах	Катренко А.В.	

11. Зміни та доповнення до робочої програми навчальної дисципліни

№ з/п	Зміст внесених змін (доповнень)	Дата і № протоколу засідання кафедри	Примітки
1			
...			
N			