МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КАФЕДРА ІНФОРМАЦІЙНОЇ ЕКОНОМІКИ, ПІДПРИЄМНИЦТВА ТА ФІНАНСІВ

ЗАТВЕРДЖУЮ

Директор Інженерного навчально-наукового інституту ЗНУ

_____ Н.Г. Метеленко
(підпис) (ініціали та прізвище)

«26» серпня 2021 р.

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ
РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

підготовки бакалавра
очної (денної) та заочної (дистанційної) форм здобуття освіти
спеціальності **051 Економіка**
освітньо-професійна програма «Інформаційна економіка»

Укладач **Клопов І. О.,** доктор економічних наук, доцент, доцент кафедри інформаційної економіки, підприємництва та фінансів

Обговорено та ухвалено
на засіданні кафедри інформаційної економіки, підприємництва та фінансів

Протокол № 1 від «27» серпня 2021 р.
Завідувач кафедри

_____ В.В. Глущевський
(підпис) (ініціали, прізвище)

Ухвалено науково-методичною радою
Інженерного навчально-наукового інституту ЗНУ
Протокол № 1 від «26» серпня 2021 р.
Голова науково-методичної ради
Інженерного навчально-наукового інституту ЗНУ

_____ Т.А. Шарапова
(підпис) (ініціали, прізвище)

Погоджено
з навчально-методичним відділом

_____ О.В. Меликівська
(підпис) (ініціали, прізвище)

2021 рік

1. Опис навчальної дисципліни

<table>
<tr><th>1</th><th>2</th><th colspan="2">3</th></tr>
<tr><td rowspan="2">Галузь знань, спеціальність, освітня програма
рівень вищої освіти</td><td rowspan="2">Нормативні показники для планування і розподілу дисципліни на змістові модулі</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>очна (денна) форма здобуття освіти</td><td>заочна (дистанційна) форма здобуття освіти</td></tr>
<tr><td rowspan="2">Галузь знань
05 «Соціальні та поведінкові науки»</td><td rowspan="2">Кількість кредитів – 5</td><td colspan="2">Обов’язкова</td></tr>
<tr><td colspan="2">Цикл дисциплін
Професійної підготовки освітньої програми</td></tr>
<tr><td>Спеціальність
051 «Економіка»</td><td rowspan="2">Загальна кількість годин – 150</td><td colspan="2">Семестр:</td></tr>
<tr><td rowspan="3">Освітньо-професійна програма
«Інформаційна економіка»</td><td>2 -й</td><td>2 -й</td></tr>
<tr><td rowspan="3">Змістових модулів – 8</td><td colspan="2">Лекції</td></tr>
<tr><td>32 год.</td><td>6 год.</td></tr>
<tr><td rowspan="4">Рівень вищої освіти:
бакалаврський</td><td colspan="2">Лабораторні роботи</td></tr>
<tr><td rowspan="3">Кількість поточних контрольних заходів – 16</td><td>32 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>86 год.</td><td>138 год.</td></tr>
<tr><td colspan="2">Вид підсумкового семестрового контролю:
залік</td></tr>
</table>

2. Мета та завдання навчальної дисципліни

Метою вивчення навчальної дисципліни «Інформаційна безпека та захист інформації» є формування знань і навичок, необхідних для формалізованого опису, синтезу й аналізу, криптографічних систем.

Основні ***завдання*** вивчення дисципліни «Інформаційна безпека та захист інформації» полягають в тому, щоб ознайомити студентів з основами математичних теорій, на яких ґрунтуються криптографія та криптоаналіз, і навчити їх практичному застосуванню цих основ для розв‘язання конкретних задач криптографії та криптоаналізу; ознайомити з сучасними криптографічними алгоритмами й протоколами, відомими підходами до аналізу криптосистем та тенденціями розвитку криптографії та криптоаналізу, навчити методам синтезу й аналізу криптосистем.

У результаті вивчення навчальної дисципліни студент повинен набути таких результатів навчання (знання, уміння тощо) та компетентностей:

Заплановані робочою програмою результати навчання та компетентності	Методи і контрольні заходи
1	**2**
Загальні компетентності: ЗК4. Здатність застосовувати знання у практичних ситуаціях. ЗК8. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.	Методи: Наочні методи (схеми, моделі, алгоритми). Словесні методи (лекція, пояснення, робота з підручником). Практичні методи (творчі завдання, контрольні, складання схем і алгоритмів). Логічні методи (індуктивні, дедуктивні, створення проблемної ситуації). Проблемно-пошукові методи (репродуктивні). Метод формування пізнавального інтересу (навчальна дискусія, створення цікавих ситуацій).
Спеціальні (фахові, предметні) компетентності СК2. Здатність здійснювати професійну діяльність у відповідності з чинними нормативними та правовими актами. СК7. Здатність застосовувати комп’ютерні технології та програмне забезпечення з обробки даних для вирішення економічних завдань, аналізу інформації та підготовки аналітичних звітів. СК14. Здатність поглиблено аналізувати проблеми і явища в одній або декількох	Методи: Дослідницький (самостійна робота, проекти). Наочні методи (схеми, моделі, алгоритми). Проблемно-пошукові методи (репродуктивні). Практичні методи (творчі завдання, контрольні, складання схем і алгоритмів). Логічні методи (індуктивні, дедуктивні, створення проблемної

професійних сферах з врахуванням економічних ризиків та можливих соціально-економічних наслідків. СК 15. Розуміння принципів, функцій і домінант інформаційної економіки як особливої та самостійної парадигми світового економічного світогляду. СК 18. Навички використання пакетів прикладних програм, прикладного комп'ютерного програмного забезпечення, спеціалізованих цифрових сервісів для вирішення задач аналізу і синтезу соціально-економічних, математичних, інформаційних та інших складних систем.	ситуації). Метод формування пізнавального інтересу (навчальна дискусія, створення цікавих ситуацій). Контрольні заходи: – теоретичне тестування за змістовим модулем.
Програмні результати навчання: ПРН4. Розуміти принципи економічної науки, особливості функціонування економічних систем. ПРН5. Застосовувати аналітичний та методичний інструментарій для обґрунтування пропозицій та прийняття управлінських рішень різними економічними агентами (індивідуумами, домогосподарствами, підприємствами та органами державної влади). ПРН7. Пояснювати моделі соціально-економічних явищ з погляду фундаментальних принципів і знань на основі розуміння основних напрямів розвитку економічної науки. ПРН8. Застосовувати відповідні економіко-математичні методи та моделі для вирішення економічних задач. ПРН10. Проводити аналіз функціонування та розвитку суб'єктів господарювання, визначати функціональні сфери, розраховувати відповідні показники які характеризують результативність їх діяльності. ПРН13. Ідентифікувати джерела та розуміти методологію визначення і методи отримання соціально-економічних даних, збирати та аналізувати необхідну інформацію, розраховувати економічні та соціальні показники. ПРН17. Виконувати міждисциплінарний аналіз соціально- економічних явищ і проблем в однієї або декількох професійних сферах з врахуванням ризиків та можливих соціально-економічних наслідків. ПРН 19. Використовувати інформаційні та комунікаційні технології для вирішення соціально-економічних завдань, підготовки та представлення аналітичних звітів.	Методи контролю і самоконтролю (усний, письмовий, програмований, лабораторно-практичний). Самостійно-пошукові методи (індивідуальна робота, практична робота). Контрольні заходи: – захист індивідуальних лабораторних робіт; – теоретичне тестування за змістовим модулем. – залік.

ПРН 25. Проводити системний аналіз реальних об'єктів інформатизації, обґрунтовувати вибір інформаційних і комунікаційних технологій для комп'ютерної реалізації їх інформаційних моделей з врахуванням ризиків інформаційної безпеки та кібербезпеки. ПРН 30. Застосовувати міждисциплінарні методи дослідження на стику економіки, менеджменту, математики, інформатики та інших наук і відповідні прикладні інформаційні та комунікаційні системи й технології для вирішення завдань інформатизації управлінської діяльності економічних систем.	

Міждисциплінарні зв'язки. Вивчення навчальної дисципліни «Інформаційна безпека та захист інформації» є логічним продовженням курсу «Вступ за фахом «Інформаційна економіка»». Набуті при вивченні даного курсу знання необхідні для подальшого вивчення курсів: «Управлінська діяльність підприємства», «Економіка підприємства», «Фінанси», «Методи та моделі штучного інтелекту» та подальшої дослідницької діяльності в інформаційній економіці та інших галузях науки та техніки.

3. Програма навчальної дисципліни

Змістовий модуль 1. Інформаційна безпека комп'ютерних систем

Поняття інформаційної безпеки комп'ютерних систем. Апаратно-програмні засоби захисту інформації. Основні елементи політики безпеки інформаційних систем.

Змістовий модуль 2. Засоби криптографічного захисту інформації

Класифікація методів криптографічного захисту інформації. Шифрування інформації методами підстановок та перестановок. Шифрування інформації методами гамування та аналітичних перетворень. Комбіновані методи. Концепція криптосистем з відкритим ключем.

Змістовий модуль 3. Засоби криптографічного захисту інформації (продовження)

Змістовий модуль 4. Електронний цифровий підпис

Проблема аутентифікації даних та електронний цифровий підпис. Хеш-функція та особливості її використання. Алгоритм шифрування електронного цифрового підпису RSA.

Змістовий модуль 5. Захист інформаційних систем від несанкціонованого доступу

Методи захисту програм від копіювання. Методи захисту компакт-дисків від копіювання. Комп'ютерна графологія.

Змістовий модуль 6. Програми з потенційно небезпечними наслідками та технології боротьби з ними

Класифікація програм з потенційно небезпечними наслідками. Міжмережеві екрани.

Змістовий модуль 7. Комп'ютерні атаки та технології їх виявлення

Моделі комп'ютерних атак та етапи їх реалізації. Безпека систем електронної комерції. Безпека електронних платіжних систем.

Змістовий модуль 8. Загальні положення захисту інформації на основі міжнародних стандартів

Безпека інформаційних ресурсів у ІКСМ. Організація технічного захисту інформації. Методика і критерії оцінки захищеності інформації. Захист інформації на базі ISO/IEC.

4. Структура навчальної дисципліни

Змістовий модуль	Усього годин	Аудиторні (контактні) години						Самостійна робота, год		Система накопичення балів		
		Усього годин		Лекційні заняття, год		Лабораторні роботи, год				Теор. зав-ня, к-ть балів	Практ. зав-ня, к-ть балів	Усього балів
				о/д ф.	з/дист ф.	о/д ф.	з/дист ф.	о/д ф.	з/дист ф.			
1	***2***	***3***		***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***
1	15	8	-	4	-	4	-	7	15	3	4	7
2	15	8	-	4	-	4	-	7	15	3	4	7
3	15	8	2	4	1	4	1	7	13	3	4	7
4	15	8	2	4	1	4	1	7	13	3	4	7
5	15	8	2	4	1	4	1	7	13	4	4	8
6	15	8	2	4	1	4	1	7	13	4	4	8
7	15	8	2	4	1	4	1	7	13	4	4	8
8	15	8	2	4	1	4	1	7	13	4	4	8
Усього за змістові модулі	120	64	12	32	6	32	6	56	108	28	32	60
Підсумковий семестровий контроль **залік**	30									20	20	40
Загалом	**150**									**100**		

5. Теми лекційних занять

№ змістового модуля	Назва теми	Кількість годин	
		о/д ф.	з/дист ф.
1	***2***	***3***	***4***
1	Інформаційна безпека комп'ютерних систем	4	-
2	Засоби криптографічного захисту інформації	4	-
3	Засоби криптографічного захисту інформації (продовження)	4	1
4	Електронний цифровий підпис	4	1
5	Захист інформаційних систем від несанкціонованого доступу	4	1
6	Програми з потенційно небезпечними наслідками та технології боротьби з ними	4	1
7	Комп'ютерні атаки та технології їх виявлення	4	1
8	Загальні положення захисту інформації на основі міжнародних стандартів	4	1
Разом		**32**	6

6. Теми лабораторних робіт

№ змістового модуля	Назва теми	Кількість годин	
		о/д ф.	о/д ф.
1	***2***	***3***	***4***
1	Шифрування методом підстановок: одно алфавітна підстановка	4	-
2	Шифрування методом підстановок: таблиця Віжинера	4	-
3	Шифрування методом підстановок: таблиця Віжинера (продовження)	4	1
4	Шифрування методом простої перестановки	4	1
5	Шифрування методом гамування	4	1
6	Шифрування методом аналітичних перетворень	4	1
7	Криптосистеми з відкритим ключем: система RSA	4	1
8	Електронний цифровий підпис: побудова хеш-функції	4	1
Разом		**32**	**6**

7. Види і зміст поточних контрольних заходів

№ змістового модуля	Види поточних контрольних заходів	Зміст поточного контрольного заходу	Критерії оцінювання	Усього балів
1	**2**	**3**	**4**	**5**
1	Тест 1	Питання для підготовки: Поняття інформаційної безпеки комп'ютерних систем. Апаратно-програмні засоби захисту інформації. Основні елементи політики безпеки інформаційних систем.	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 10. Правильна відповідь оцінюється у 0,3 бали.	**3**
	Лабораторна робота 1	Вимоги до виконання та оформлення: Лабораторна робота у вигляді файлу завантажена на сайт системи Moodle ЗНУ.	Кожне завдання лабораторної роботи за змістовим модулем оцінюється від 1 до 4 балів з урахуванням відповідей на запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	**4**
Усього за ЗМ 1	**2**			**7**
2	Тест 2	Питання для підготовки: Класифікація методів криптографічного захисту інформації. Шифрування інформації методами підстановок та перестановок. Шифрування інформації методами гамування та аналітичних перетворень. Комбіновані методи. Концепція криптосистем з відкритим ключем.	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 10. Правильна відповідь оцінюється у 0,3 бали.	**3**
	Лабораторна робота 2	Вимоги до виконання та оформлення: Лабораторна робота у вигляді файлу завантажена на сайт системи Moodle ЗНУ.	Кожне завдання лабораторної роботи за змістовим модулем оцінюється від 1 до 4 балів з урахуванням відповідей на запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	**4**
Усього за ЗМ 2	**2**			**4**
3	Тест 3	Питання для підготовки:	Тестові питання оцінюються:	**3**

		Класифікація методів криптографічного захисту інформації. Шифрування інформації методами підстановок та перестановок. Шифрування інформації методами гамування та аналітичних перетворень. Комбіновані методи. Концепція криптосистем з відкритим ключем.	правильно/ неправильно. Кількість питань – 10. Правильна відповідь оцінюється у 0,3 бали.	
	Лабораторна робота 3	Вимоги до виконання та оформлення: Лабораторна робота у вигляді файлу завантажена на сайт системи Moodle ЗНУ.	Кожне завдання лабораторної роботи за змістовим модулем оцінюється від 1 до 4 балів з урахуванням відповідей на запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	**4**
Усього за ЗМ 3	**2**			**7**
4	Тест 4	Питання для підготовки: Проблема аутентифікації даних та електронний цифровий підпис. Хеш-функція та особливості її використання. Алгоритм шифрування електронного цифрового підпису RSA.	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 10. Правильна відповідь оцінюється у 0,3 бали.	**3**
	Лабораторна робота 4	Вимоги до виконання та оформлення: Лабораторна робота у вигляді файлу завантажена на сайт системи Moodle ЗНУ.	Кожне завдання лабораторної роботи за змістовим модулем оцінюється від 1 до 4 балів з урахуванням відповідей на запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	**4**
Усього за ЗМ 4	**2**			**7**
5	Тест 5	Питання для підготовки: Методи захисту програм від копіювання. Методи захисту компакт-дисків від копіювання. Комп'ютерна графологія.	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 10. Правильна відповідь оцінюється у 0,4 бали.	**4**
	Лабораторна робота 5	Вимоги до виконання та оформлення: Лабораторна робота у вигляді файлу завантажена на сайт системи Moodle	Кожне завдання лабораторної роботи за змістовим модулем оцінюється від 1 до 4 балів з урахуванням відповідей на	**4**

		ЗНУ.	запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	
Усього за ЗМ 5	**2**			**8**
6	Тест 6	Питання для підготовки: Класифікація програм з потенційно небезпечними наслідками. Міжмережеві екрани.	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 10. Правильна відповідь оцінюється у 0,4 бали.	**4**
	Лабораторна робота 6	Вимоги до виконання та оформлення: Лабораторна робота у вигляді файлу завантажена на сайт системи Moodle ЗНУ.	Кожне завдання лабораторної роботи за змістовим модулем оцінюється від 1 до 4 балів з урахуванням відповідей на запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	**4**
Усього за ЗМ 6	**2**			**8**

7	Тест 7	Питання для підготовки: Моделі комп'ютерних атак та етапи їх реалізації. Безпека систем електронної комерції. Безпека електронних платіжних систем.	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 10. Правильна відповідь оцінюється у 0,4 бали.	**4**
	Лабораторна робота 7	Вимоги до виконання та оформлення: Лабораторна робота у вигляді файлу завантажена на сайт системи Moodle ЗНУ.	Кожне завдання лабораторної роботи за змістовим модулем оцінюється від 1 до 4 балів з урахуванням відповідей на запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	**4**
Усього за ЗМ 7	**2**			**8**
8	Тест 8	Питання для підготовки: Безпека інформаційних ресурсів у ІКСМ. Організація технічного захисту інформації. Методика і критерії оцінки захищеності інформації. Захист інформації на базі ISO/IEC.	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 10. Правильна відповідь оцінюється у 0,4 бали.	**4**
	Лабораторна робота 8	Вимоги до виконання та оформлення:	Кожне завдання лабораторної роботи за	**4**

		Лабораторна робота у вигляді файлу завантажена на сайт системи Moodle ЗНУ.	змістовим модулем оцінюється від 1 до 4 балів з урахуванням відповідей на запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	
Усього за ЗМ 8	**2**			**8**
Усього за змістові модулі	**16**			**60**

8. Підсумковий семестровий контроль

Форма	Види підсумкових контрольних заходів	Зміст підсумкового контрольного заходу	Критерії оцінювання	Усього балів
1	**2**	**3**	**4**	**5**
Залік	**Тестування**	Питання для підготовки: див. питання до ЗМ 1–8 у таблиці 7. Тестування передбачає обмежену у часі (40 хвилин) відповідь на теоретичні питання. У разі дистанційної форми навчання залік проходить у тестовій формі через платформу Moodle.	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 20. Правильна відповідь оцінюється у 1 бал.	**20**
	Розв'язання задачі	Підсумкове практичне завдання	Задача складається з 2 практичних завдань, за кожне з яких студент може отримати до 10 балів, з урахуванням відповідей на запитання при захисті роботи.	**20**
Усього за підсумковий семестровий контроль	**2**			**40**

9. Рекомендована література

Основна:

1. Лужецький В. А. Основи інформаційної безпеки : навчальний посібник. Черкаси: ЧДТУ, 2018. 223 с.
2. Технології захисту інформації: підручник для студ. / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2018. 162 с.
3. Al Sweigart Cracking Codes with Python. An Introduction to Building and Breaking Ciphers. Al Sweigart, 2018. 416 p.

Додаткова:

1. Лужецький В. А. Інформаційна безпека : навчальний посібник. Вінниця : УНІВЕРСУМ-Вінниця. 2019. 240 с.
2. Лужецький В. А. Захист персональних даних : навчальний посібник. Вінниця : УНІВЕРСУМ-Вінниця, 2017. 248 с.
3. Грайворонський М. В. Безпека інформаційно-комунікаційних систем. Київ : Вид.група BUV, 2019. 608 с.
4. Лісовська Ю. П. Інформаційна безпека України : навчальний посібник для студентів вищих навчальних закладів. Київ : Кондор, 2020. 170 с.
5. Sean Smith The Internet of Risky Things: Trusting the Devices That Surround Us 1st Edition. O'Reilly Media. 2017. 240 p.

Інформаційні ресурси:

1. Закон України «Про інформацію» : за станом на 1 січня 2013 р. / Верховна Рада України. Офіц. вид. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» : за станом на 1 січня 2013 р. / Верховна Рада України. Офіц. вид. URL: http://zakon.rada.gov.ua/cgi- bin/laws/main.cgi?nreg=80%2F94-%E2%F0
3. Портал безпека [Електронний ресурс]. URL : www.bezpeka.com
4. Національна бібліотека України імені В. І. Вернадського. URL: http://www.nbuv.gov.ua/

Додаток

Доповнення та зміни до робочої програми навчальної дисципліни

«_____»

(назва)

Протокол засідання кафедри (дата та номер)	Внесені зміни	Підпис завідувача кафедри, дата