МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАЗМІСТОВИЙ МОДУЛЬТИЧНИЙ ФАКУЛЬТЕТ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ЗАТВЕРДЖУЮ
Декан математичного
факультету
_____С.І. Гоменюк
"_____"_____2020 р.

ОСНОВИ КРИПТОЛОГІЇ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

підготовки _____бакалаврів_____
(назва освітнього ступеня)
очної (денної) та заочної (дистанційної) форм здобуття освіти
спеціальності __122 комп'ютерні науки_____
(шифр, назва спеціальності)
спеціалізації / предметної спеціальності _____
(шифр і назва)
освітньо-професійна програма__комп'ютерні науки_____

Укладач Решевська К.С. к.т.н.,
доцент, доцент кафедри
комп'ютерних наук

Обговорено та ухвалено
на засіданні кафедри комп'ютерних наук
Протокол №5 від «16» листопада 2020р.
Завідувач кафедри
_____С.Ю. Борю

Ухвалено науково-методичною радою маЗмістовий модультичного факультету

Протокол № від « » _____2020 р.

Голова науково-методичної ради факультету

_____О.С. Пшенична

Погоджено
з навчально-методичним відділом

_____
(підпис) (ініціали, прізвище)

Погоджено з навчальною лабораторією інформаційного забезпечення освітнього процесу

_____
(підпис) (ініціали, прізвище)

2020 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
0403 – Системні науки та кібернетика</td><td rowspan="2">Кількість кредитів – 5</td><td colspan="2">Вибіркова</td></tr>
<tr><td colspan="2">Цикл дисциплін вільного вибору студента в межах спеціальності</td></tr>
<tr><td>Спеціальність
122 комп’ютерні науки</td><td rowspan="2">Загальна кількість годин – 150</td><td colspan="2">Семестр:</td></tr>
<tr><td rowspan="2">Спеціалізація
_____
(шифр і назва)</td><td>8-й</td><td>10-й</td></tr>
<tr><td rowspan="2">Освітньо-професійна програма
комп’ютерні науки</td><td rowspan="2">*Змістових модулів – 8</td><td colspan="2">Лекції</td></tr>
<tr><td>24 год.</td><td>6 год.</td></tr>
<tr><td rowspan="4">Рівень вищої освіти:
бакалаврський
(необхідне обрати)</td><td rowspan="4">Кількість поточних контрольних заходів – 8</td><td colspan="2">Практичні</td></tr>
<tr><td>36 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>90 год.</td><td>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 «Основи криптології» є засвоєння маЗмістовий модультичних та термінологічних основ з криптології, вивчення студентами процесу проведення аналізу погроз безпеці інформації, основних методів, механізмів, алгоритмів та протоколів криптографічного захисту інформації в інформаційно-комунікаційних сисЗмістовий модульх з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз та проведення криптографічного аналізу зі сторони потенційних порушників.

Основними **завданнями** вивчення дисципліни «Основи криптології» є: формування у студентів певних професійних компетенцій, знань та вмінь з теорії та практики криптографічного захисту інформації та криптографічного аналізу.

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Згідно вимогам освітньої програми студенти повинні досягти таких результатів навчання.

знання:

— канали уразливості та витоку інформації, явища, що притаманні їх прояву та існуванню;

— основні методи, механізми, протоколи та алгоритми криптографічного захисту інформації;

— критерії та показники оцінки якості криптографічного захисту інформації;

— методи криптографічних перетворень інформації та способи їх здійснення;

— методи та засоби аналізу та криптоаналізу асиметричних та симетричних крипто перетворень;

уміння:

— обґрунтовувати, вибирати та застосовувати критерії та показники оцінки стійкості криптографічних перетворень та безпечності криптографічних протоколів;

— обґрунтовувати, вибирати та застосовувати критерії та показники оцінки стійкості криптографічних перетворень та безпечності криптографічних протоколів;

— розробляти вимоги та обирати для застосування криптографічні перетворення та протоколи, що мінімізують впливи порушників;

— розробляти моделі загроз безпеці інформації, вирішувати завдання аналізу та синтезу криптографічних алгоритмів та протоколів захисту інформації;

— моделювати крипто аналітичні атаки та здійснювати крипто аналіз;

— аналізувати криптографічні протоколи на їх рівень безпечності (повноту, коректність та нульове розголошення тощо);

— оцінювати захищеність від несанкціонованого доступу до інформації;

— обґрунтовувати вимоги до ключових даних та ключової інформації, здійснювати аналіз їх властивостей;

— застосовувати стандартні пакети при розв’язанні прикладних задач моделювання криптографічних перетворень, ключових даних та протоколів;

— використовувати маЗмістовий модультичний апарат для освоєння теоретичних основ і практичного використання криптографічних методів;

— використовувати професійно профільовані знання й практичні навички в галузі маЗмістовий модультики, маЗмістовий модультичного аналізу для освоєння загальної та прикладної криптографії;

— володіляти спеціалізованими програмними пакетами;

компетентності:

– **ЗК1** Здатність до абстрактного мислення, аналізу та синтезу

– **ЗК3** Знання та розуміння предметної області та розуміння професійної діяльності

– **ЗК6** Здатність вчитися і оволодівати сучасними знаннями

– **СК3** Здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності, розв'язності та нерозв'язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем

– **СК4** Здатність використовувати сучасні методи маЗмістовий модультичного моделювання об'єктів, процесів і явищ, розробляти моделі й алгоритми чисельного розв'язування задач маЗмістовий модультичного моделювання, враховувати похибки наближеного чисельного розв'язування професійних задач

– **СК8** Здатність проектувати та розробляти програмне забезпечення із застосуванням різних парадигм програмування: узагальненого, об'єктно-орієнтованого, функціонального, логічного, з відповідними моделями, методами й алгоритмами обчислень, структурами даних і механізмами управління

– **СК11** Здатність до інтелектуального аналізу даних на основі методів обчислювального інтелекту включно з великими та погано структурованими даними, їхньої оперативної обробки та візуалізації результатів аналізу в процесі розв'язування прикладних задач

– **СК13** Здатність до розробки мережевого програмного забезпечення, що функціонує на основі різних топологій структурованих кабельних систем, використовує комп'ютерні системи і мережі передачі даних та аналізує якість роботи комп'ютерних мереж

– **СК14** Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури

Заплановані робочою програмою результати навчання та компетентності	Методи і контрольні заходи
1	**2**
ЗК 1, 3, 6, СК 3,4,8,11,13,14	**Методи навчання**: лекційний метод, лекція-візуалізація, дискусія, аналітичний, метод проектів (індивідуальні), моделювання, виконання завдань, , виконання лабораторних робіт. **Методи контролю**: опитування, тестування, захист лабораторної роботи, оцінювання звіту.

Міждисциплінарні зв'язки.

Дисципліна «Основи криптології» вимагає від студентів знань та умінь з дисциплін циклу професійної підготовки освітньої програми, а саме:

1. «Об'єктно-орієнтоване програмування»
2. «Процедурне програмування»

3. Програма навчальної дисципліни

Змістовий модуль 1. Основи теорії секретних систем.
Основні терміни. Вимоги до криптографічних систем. Принципи побудови й схеми криптологічних систем. Класифікація алгоритмів шифрування

Змістовий модуль 2. Симетричні криптографічні перетворення та їх властивості
Класифікація симетричних криптографічних перетворень. Основні елементарні крипто перетворення симетричного типу. Криптографічні перетворення (шифри) типу перестановка та підстановка. Криптографічні перетворення (шифри) типу зсув символів.

Змістовий модуль 3. Блочні шифри та режими їх роботи.
Поняття блочного шифру. Структура та види алгоритмів блочного типу. Електронна кодова книга. Сцеплення блоків шифру. Зворотній зв'язок за шифртекстом. Зворотній зв'язок за виходом.

Змістовий модуль 4. Мережі Фейстеля. **SP – мережі та системи класу «квадрат»**
Структура алгоритму на основі мережі Фейстеля. Алгоритми, що засновані на мережі Фейстеля. Алгоритми на основі підстановочно-перестановочних мереж. Приклади.

Змістовий модуль 5. Вступ в теорію асиметричних крипто перетворень

Вступ в теорію асиметричних криптоперетворень. Алгоритм Діфі-Хелмана. Джерела ключів асиметричних криптосистем та вимоги до них. Методи крипто аналізу асиметричних криптосистем. Алгоритм RSA та його криптоаналіз. Приклади використання. Використання систем дискретного логарифму упри шифруванні даних. Приклади використання

Змістовий модуль 6.Алгоритми підписання та перевірки ЕЦП

Огляд алгоритмів ЕЦП. ЕЦП засновані на алгоритмах Діфі-Хелмана та Ель Гамаля.

Змістовий модуль 7. Хеш-функції та методи аутентифікації

Кріптографічні хеш-функції. Застосування хеш-функцій для перевірки істинності повідомлення. Схема Маркеля-Дамгарда. Типи криптографічних функцій.

Змістовий модуль 8. Криптоаналіз асиметричних алгоритмів

Методи крипто аналізу асиметричних криптосистем. Методи та алгоритми крипто аналізу криптографічних перетворень в групі точок еліптичних кривих.

4. Структура навчальної дисципліни

Змістовий модуль	Усього годин	Аудиторні (контактні) години					Самостійна робота, год		СисЗмістовий модуль накопичення балів		
		Усього годин	Лекційні заняття, год		Практичні, 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**	**10**	4	2	6	2	5	**11**	**3**	**3**	**6**
2	**15**	**8**	2	2	6	2	7	**11**	**3**	**4**	**7**
3	**15**	**8**	2		6		7	**15**	**3**	**4**	**7**
4	**15**	**4**	4				11	**15**	**5**	**5**	**10**
5	**15**	**10**	4	2	6	2	5	**11**	**3**	**3**	**6**
6	**15**	**8**	2		6		7	**15**	**3**	**4**	**7**
7	**15**	**10**	4		6		5	**15**	**3**	**4**	**7**
8	**15**	**2**	2				13	**15**	**5**	**5**	**10**
Усього за змістові модулі	**120**	**56**	24	6	36	6	**60**	**108**	**28**	**32**	60
Підсумковий семестровий контроль **Залік**	30						30				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	Основи теорії секретних систем	4	2
2	Симетричні криптографічні перетворення та їх властивості	2	2
3	Блочні шифри та режими їх роботи	2	
4	Мережі Фейстеля. SP – мережі та системи класу «квадрат»	4	
5	Вступ в теорію асиметричних крипто перетворень	4	2
6	Алгоритми підписання та перевірки ЕЦП	2	
7	Хеш-функції та методи аутентифікації	4	
8	Криптоаналіз асиметричних алгоритмів	2	
Разом		24	6

6. Теми практичних занять

№ змістового модуля	Назва теми	Кількість годин	
		о/д ф.	з/дист ф.
1	**2**	**3**	**4**
1	Класичні криптосистеми	6	2
2	Блочні шифри. Алгоритм DES	6	2
3	Алгоритм шифрування AES	6	
4	Системи шифрування з відкритим ключем	6	2
5	ЕЦП на основі алгоритму Діфі-Хелмана	6	
6	ЕЦП на основі алгоритму Ель-Гамаля	6	
Разом		36	6

7. Види і зміст поточних контрольних заходів *

№ змістового модуля	Вид поточного контрольного заходу	Зміст поточного контрольного заходу	**Критерії оцінювання	Усього балів
1	**2**	**3**	**4**	**5**
1	Теоретичне завдання	Питання для підготовки: https://moodle.znu.edu.ua/course/view.php?id=4199	1 бал за кожну вірну відповідь на одне теоретичне питання зі списку питань до практичної роботи	**3**
	Практичне завдання	Вимоги до виконання та оформлення: https://moodle.znu.edu.ua/course/view.php?id=4199	3 бали при виконанні завдань з практичної роботи №1	**3**
Усього за ЗМ 1 контр. заходів	**1**			**6**
2	Теоретичне завдання	Питання для підготовки: https://moodle.znu.edu.ua/course/view.php?id=4199	1 бал за кожну вірну відповідь на одне теоретичне питання зі списку питань до практичної роботи №2	**3**
	Практичне завдання	Вимоги до виконання та оформлення: https://moodle.znu.edu.ua/course/view.php?id=4199	4 бали при виконанні завдань з практичної роботи №2	**4**
Усього за ЗМ 2 контр. заходів	**1**			**7**
3	Теоретичне завдання	Питання для підготовки: https://moodle.znu.edu.ua/course/view.php?id=4199	1 бал за кожну вірну відповідь на одне теоретичне питання зі списку питань до практичної роботи №3	**3**
	Практичне завдання	Вимоги до виконання та оформлення: https://moodle.znu.edu.ua/course/view.php?id=4199	4 бали при виконанні завдань з практичної роботи №3	**4**
Усього за ЗМ 3 контр. заходів	1			**7**

4	Теоретичне завдання	Питання для підготовки: https://moodle.znu.edu.ua/course/view.php?id=4199	1 бал за кожну вірну відповідь на одне теоретичне питання тесту	**5**
	Практичне завдання – практичні завдання	Вимоги до виконання та оформлення: https://moodle.znu.edu.ua/course/view.php?id=4199	1 бал за кожну вірну відповідь на одне практичне питання тесту	**5**
Усього за ЗМ 4 контр. заходів	1			**10**
5	Теоретичне завдання	Питання для підготовки: https://moodle.znu.edu.ua/course/view.php?id=4199	1 бал за кожну вірну відповідь на одне теоретичне питання зі списку питань до практичної роботи №4	**3**
	Практичне завдання	Вимоги до виконання та оформлення: https://moodle.znu.edu.ua/course/view.php?id=4199	3 бали при виконанні завдань з практичної роботи №4	**3**
Усього за ЗМ 5 контр. заходів	1			**6**
6	Теоретичне завдання	Питання для підготовки: https://moodle.znu.edu.ua/course/view.php?id=4199	1 бал за кожну вірну відповідь на одне теоретичне питання зі списку питань до практичної роботи № 5	**3**
	Практичне завдання	Вимоги до виконання та оформлення: https://moodle.znu.edu.ua/course/view.php?id=4199	4 бали при виконанні завдань з практичної роботи №5	**4**
Усього за ЗМ 6 контр. заходів	1			**7**
7	Теоретичне завдання	Питання для підготовки: https://moodle.znu.edu.ua/course/view.php?id=4199	1 бал за кожну вірну відповідь на одне теоретичне питання зі списку питань до практичної роботи №6	**3**
	Практичне завдання	Вимоги до виконання та оформлення: https://moodle.znu.edu.ua/course/view.php?id=4199	4 бали при виконанні завдань з практичної роботи №6	**4**

Усього за ЗМ 7 контр. заходів	1			**7**
8	Теоретичне завдання	Питання для підготовки: https://moodle.znu.edu.ua/course/view.php?id=4199	1 бал за кожну вірну відповідь на одне теоретичне питання тесту №2	**5**
	Практичне завдання	Вимоги до виконання та оформлення: https://moodle.znu.edu.ua/course/view.php?id=4199	1 бал за кожну вірну відповідь на одне практичне питання тесту №2	**5**
Усього за ЗМ 8 контр. заходів	**1**			**10**
Усього за змістові модулі контр. заходів	**8**			**60**

8. Підсумковий семестровий контроль

Форма	Види підсумкових контрольних заходів	Зміст підсумкового контрольного заходу	Критерії оцінювання	Усього балів
1	**2**	**3**	**4**	**5**
Екзамен	Теоретичне завдання	Питання для підготовки: https://moodle.znu.edu.ua/course/view.php?id=4199	1 бал за вірну відповідь підсумкового тесту	**20**
	Практичне завдання	Індивідуальне завдання: https://moodle.znu.edu.ua/mod/assign/view.php?id=4199	https://moodle.znu.edu.ua/mod/assign/view.php?id=4199	**20**
Усього за підсумковий семестровий контроль				**40**

9. Рекомендована література

Основна:

1. Корченко О.Г., Сіденко В.П., Дрейс Ю.О. Прикладна криптологія: системи шифрування. Житомир : Державниий університет телекомунікацій (ДУТ), 2015. 448 с.

2. Іваночко С.Г. Криптологія. Львів: Національний Університет Львівська Політехніка, 2018. 46 с.

3. Гребенніков В.В. Історія криптології & секретного зв'язку Ужгород: Ліра, 2015. — 664 с.

Додаткова:

4. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2015 - 368 с.

5. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків. Форт. 2018 , 593с.

Інформаційні ресурси:

1. Moodle сторінка дисципліни: https://moodle.znu.edu.ua/course/view.php?id=4199
2. Методи і засоби захисту інформації: http://citforum.ru/internet/infsecure/
3. Порівняння симетричних та асиметричних криптосистем: https://sites.google.com/site/sucasnikriptosistemik/home/porivnanna-simetricnih-z-asimetricnimi-kriptosistemami
4. Криптографія у Java: https://habr.com/ru/post/444764/
5. Ктриптографічні бібліотеки Java: http://java-online.ru/javax-crypto.xhtml

6. Криптографія з Python: https://coderlessons.com/tutorials/python-technologies/izuchite-kriptografiiu-s-python/kriptografiia-s-python-kratkoe-rukovodstvo
7. Криптографія на Python: https://habr.com/ru/post/265309/
8. Шифрування у Python: https://python-scripts.com/encryption-cryptography
9. Практичні схеми реалізації алгоритмів електронного цифрового підпису:https://www.researchgate.net/publication/328828732_PRAKTICNI_SHEMI_REALIZACII_ALGORITMIV_ELEKTRONNOGO_CIFROVOGO_PIDPISU
10. Схема ЕЦП: https://xakep.ru/2016/12/15/crypto-part5/