МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ФАХОВИЙ КОЛЕДЖ ПРОМИСЛОВОЇ АВТОМАТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ОДЕСЬКОГО НАЦІОНАЛЬНОГО ТЕХНОЛОГІЧНОГО УНІВЕРСИТЕТУ»

ЗАТВЕРДЖУЮ
Заступник директора з
навчально-методичної роботи
ФКПАІТ ОНТУ
_____ Вікторія ОКСАНІЧЕНКО
_____._____.2022 року

РОБОЧА ПРОГРАМА НОРМАТИВНОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ
(шифр за ОПП і назва навчальної дисципліни)

галузі знань 12 «Інформаційні технології»
(шифр і назва галузі знань)

спеціальності 122 «Комп'ютерні науки»
(шифр і назва спеціальності)

освітня програма Комп'ютерні науки
(назва освітньої програми)

(Шифр за ОПП ОК **)**

Одеса
2022 рік

Робоча програма «Технології захисту інформації» для підготовки фахового молодшого бакалавра за спеціальністю 122 «Комп'ютерні науки».

Укладач: викладач вищої категорії ФКПАІТ ОНТУ Юлія БУРМАКІНА

Робоча програма затверджена на засіданні циклової комісії ФКПАІТ ОНТУ_____ «Комп'ютерних наук та інженерії програмного забезпечення»

Протокол від ___._____.2022 року №___

Голова циклової комісії «Комп'ютерних наук та інженерії програмного забезпечення»

_____ Тетяна КОСТИРЕНКО
(підпис) (власне ім'я та прізвище)
___._____.2022 року

Погоджено: методист _____ Надія ТИРИЩУК
(підпис) (власне ім'я та прізвище)

Схвалено методичною радою Фахового коледжу промислової автоматики та інформаційних технологій Одеського національного технологічного університету

Протокол від ___._____.2022 року №___

___._____.2022 року _____ Вікторія ОКСАНІЧЕНКО
(підпис) (власне ім'я та прізвище)

Термін дії програми продовжено

на 20___- 20___навчальний рік _____Вікторія ОКСАНІЧЕНКО
(підпис) (власне ім'я та прізвище)

на 20___- 20___навчальний рік _____Вікторія ОКСАНІЧЕНКО
(підпис) (власне ім'я та прізвище)

на 20___- 20___навчальний рік _____Вікторія ОКСАНІЧЕНКО
(підпис) (власне ім'я та прізвище)

на 20___- 20___навчальний рік _____Вікторія ОКСАНІЧЕНКО
(підпис) (власне ім'я та прізвище)

ДОПОВНЕННЯ І ЗМІНИ ДО РОБОЧОЇ ПРОГРАМИ

1. на 20____- 20____навчальний рік

   До змістового модуля №_____

2. на 20____- 20____навчальний рік

   До змістового модуля №_____

3. на 20____- 20____навчальний рік

   До змістового модуля №_____

4. на 20____- 20____навчальний рік

   До змістового модуля №_____

1 Опис навчальної дисципліни

<table>
<tr><th>Найменування показників</th><th>Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th colspan="2">Характеристика навчальної дисципліни
денна форма навчання</th></tr>
<tr><td>Кількість кредитів – 3</td><td>Галузь знань
12 Інформаційні технології</td><td colspan="2">Нормативна</td></tr>
<tr><td>Блоків модулів – 2</td><td rowspan="3">Спеціальність:
122 «Комп’ютерні науки»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів - 2</td><td>4-й</td><td></td></tr>
<tr><td rowspan="2">Загальна кількість годин – 90</td><td colspan="2">Семестр</td></tr>
<tr><td>7-й</td><td></td></tr>
<tr><td rowspan="8">У тому числі:
аудиторних – 52 годин
самостійної роботи студента – 38 годин</td><td rowspan="8">Освітньо-кваліфікаційний рівень:
Фаховий молодший бакалавр</td><td colspan="2">Лекції</td></tr>
<tr><td colspan="2">38 годин</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td colspan="2">14 годин</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td colspan="2">38 годин</td></tr>
<tr><td colspan="2">Вид підсумкового контролю з дисципліни:
залік</td></tr>
</table>

Примітка. Співвідношення кількості годин аудиторних занять до самостійної роботи становить відповідно: 58,5% та 41,5%.

2 Навчальна та виховна мета вивчення навчальної дисципліни

Метою вивчення навчальної дисципліни є оволодіння студентами теоретичних знань та набуття практичних навиків з дисципліни технології захисту інформації, необхідного для спеціальної підготовки та майбутньої професійної діяльності.

3 Завдання навчальної дисципліни

Основними завданнями вивчення дисципліни є формування у студентів базових уявлень про кодування та основи захисту інформації; інтелектуальний розвиток особистості, розвиток у студентів логічного мислення і просторової уяви, алгоритмічної, інформаційної та графічної культури, пам'яті, уваги, інтуїції; формування у студентів компетенцій за фахом.

4 Основні знання, що набувають студенти при вивченні дисципліни:

- Загальні поняття захисту інформації та інформаційної безпеки, джерела і способи дії загроз на об'єкти інформаційної безпеки;
- Класичні та сучасні криптографічні системи захисту інформації та вміння застосування криптографічних алгоритмів на практиці.

5 Основні вміння і навички, які набувають студенти при вивченні дисципліни:

- Використовувати практичні навички організації захисту інформації у системах збереженні даних;
- Вміти реалізувати на практиці захист інформації з використанням симетричних, асиметричних криптографічних систем та електронного цифрового підпису;
- Оцінити переваги та недоліки різних методів криптографічного захисту інформації.

6 Рекомендована література

6.1 Основна література

- Єсин В. І., Кузнєцов А. А., Сорока Л. С. Безпека інформаційних систем та технологій – Х.:ООО «ЕДЕНА», 2010.-656с.
- Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.
- Домарев В. В. Безпека інформаційних технологій: Системний підхід: - К.: ООО "ТІД ДС", 2004. – 992с.

7 Графік виконання робочої програми

Курс навчання	**1**		**2**		**3**		**4**		**Всього**
Семестр	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	
Повний обсяг часу на предмет							90		90
У тому числі аудиторних занять							52		52
з них:									
Лекції							38		38
Лабораторні							-		-
Практичні							14		14
Семінарські							-		-
консультації							-		-
Види індивідуальних завдань (РГР, КР)							-		-
Обсяг часу на самостійну роботу студента							38		38
Підсумкові форми контролю							залік		залік

8 Методи навчання

Методи організації і здійснення навчально-пізнавальної діяльності: наочні, практичні (за тематикою навчального курсу); пошукові, дослідницькі, проблемні (за характером навчально-пізнавальної діяльності).

9 Методи контролю

Методи контролю за ефективністю навчально-пізнавальної діяльності: усні, письмові перевірки знань (контрольні та модульні роботи) і самоперевірки результативності оволодіння знаннями, уміннями і навичками.

10 Програма навчальної дисципліни

Назви змістових модулів і тем	Кількість годин денна форма у тому числі						Аудіовізуальне, комп'ютерне та інше оснащення занять	Основні знання і вміння за темою	Домашнє завдання	Перелік літератури	Календарні строки проведення занять
	усього	лекції	практичні	лабораторні	семінарські	самостійна робота					
Блок змістових модулів 1 – Основі положення											
Змістовий модуль 1.1 Основні положення											
Поняття інформаційної безпеки.	**2**	2						Ознайомитися з поняттями й визначенням курсу, розглянути актуальність проблеми захисту інформації й визначити необхідність її для комп'ютерних систем.	конспект		
Інформаційна безпека комп'ютерних систем. Основні поняття і визначення.	**2**					2		Знати основні поняття і визначення.інформаційної безпеки комп'ютерних систем. поняття.	конспект, контрольні питання		
Основні поняття і положення захисту інформації в комп'ютерних системах. Об'єкти захисту інформації	**2**	2						Знати поняття та завдання захисту інформації користувача	конспект		
Основні погрози безпеки АСОІ.	**2**					2		Знати основні погрози безпеки АСОІ. Забезпечення безпеки АСОІ.	конспект, контрольні питання		
Забезпечення безпеки АСОІ	**2**					2		Забезпечення безпеки АСОІ	конспект, контрольні питання		
Принципи криптографічного захисту. Класифікація методів	**2**	2						Знати та розуміти поняття, термінологію та основні принципи криптографії та криптографічних систем.	конспект		

Назви змістових модулів і тем	Кількість годин денна форма у тому числі						Аудіовізуальне, комп'ютерне та інше оснащення занять	Основні знання і вміння за темою	Домашнє завдання	Перелік літератури	Календарні строки проведення занять
	усього	лекції	практичні	лабораторні	семінарські	самостійна робота					
криптографічного перетворення інформації.											
Разом за змістовим модулем 1.1	**12**	**6**	--	--	--	**6**					
Блок змістових модулів 2 – Методи і засоби захисту інформації в комп'ютерних системах											
Змістовий модуль 2.1 Методи і засоби захисту інформації в комп'ютерних системах											
Симетричні криптосистеми.	**2**	2						Знати про симетричні криптосистеми			
Шифри перестановки. Шифр Сцитала. Шифруючі таблиці. Шифр маршрутної перестановки. Шифр поодинокої перестановки по ключу. Метод шифрування подвійною перестановкою	**2**					2		Знати про різні шифри, а саме: шифри перестановки. шифри Сцитала, шифруючі таблиці, шифр маршрутної перестановки, шифр поодинокої перестановки по ключу, метод шифрування подвійною перестановкою			
Шифрування методом Вернама	**2**					2		Знати про шифрування методом Вернама			
Методи генерації псевдовипадкових послідовностей чисел.	**2**					2		Знати про методи генерації псевдовипадкових послідовностей чисел.			
Математичні основи криптографії	**2**					2		Знати про математичні основи криптографії			
П.р.№1 Шифри перестановки.	**2**		2					Ознайомитися з алгоритмами шифрування та дешифрування			

Назви змістових модулів і тем	Кількість годин денна форма у тому числі						Аудіовізуальне, комп'ютерне та інше оснащення занять	Основні знання і вміння за темою	Домашнє завдання	Перелік літератури	Календарні строки проведення занять
	усього	лекції	практичні	лабораторні	семінарські	самостійна робота					
Маршрутна перестановка та перестановка по ключу. Метод шифрування подвійною перестановкою								у шифрах поодинокої перестановки по ключу та подвійної перестановки.			
П.р.№1 Шифри перестановки. Маршрутна перестановка та перестановка по ключу. Метод шифрування подвійною перестановкою	**2**		2					Ознайомитися з алгоритмами шифрування та дешифрування у шифрах поодинокої перестановки по ключу та подвійної перестановки.			
Шифри заміни. Шифр Цезаря. Афінна система підстановок Цезаря. Мультиплікативна інверсія. Розширений алгоритм Евкліда. Система Цезаря з ключовим словом.	**2**	2						Ознайомитися з шифрами заміни на прикладі шифру Цезаря.			

Назви змістових модулів і тем	Кількість годин денна форма у тому числі						Аудіовізуальне, комп'ютерне та інше оснащення занять	Основні знання і вміння за темою	Домашнє завдання	Перелік літератури	Календарні строки проведення занять
	усього	лекції	практичні	лабораторні	семінарські	самостійна робота					
Нові напрямки у розвитку криптографії	**2**					2		Знати про нові напрямки у розвитку криптографії			
Криптографія і гіпотеза P≠NP	**2**					2		Знати про криптографію і гіпотезу P≠NP			
Псевдовипадкові генератори. Докази з нульовим розголошуванням.	**2**					2		Знати про псевдовипадкові генератори та докази з нульовим розголошуванням.			
П.р.№2 Шифри заміни. Шифр Цезаря. Афінна система підстановок Цезаря.	**2**		2					Ознайомитися з шифрами заміни на прикладі шифру Цезаря.			
П.р.№3 Система Цезаря з ключовим словом	**2**		2					Ознайомитися з системою Цезаря із ключовим словом.			
Шифр Полібія. Шифруючі таблиці Трисемуса.	**2**	2						Ознайомитися з алгоритмом шифрування Полібія.			
Блокові і потокові шифри	**2**					2		Знати про блокові і потокові шифри			
Режим гамування	**2**					2		Знати про режим гамування			
П.р.№4 Шифр Полібія. Шифруючі таблиці Трисемуса.	**2**		2					Ознайомитися з алгоритмом шифрування Полібія та шифруючими таблицями Трисемуса.			
Багатоалфавітні шифри. Шифр Хасегаві.	**2**	2						Ознайомитися з багатоалфавітними шифрами.			
Основні режими роботи алгоритму DES	**2**					2		Знати про основні режими роботи алгоритму DES			

Назви змістових модулів і тем	Кількість годин денна форма у тому числі						Аудіовізуальне, комп'ютерне та інше оснащення занять	Основні знання і вміння за темою	Домашнє завдання	Перелік літератури	Календарні строки проведення занять
	усього	лекції	практичні	лабораторні	семінарські	самостійна робота					
Комбінування блокових алгоритмів											
Алгоритм шифрування даних IDEA	**2**					2		Знати про алгоритм шифрування даних IDEA			
Асиметричні криптосистеми. Концепція криптосистеми з відкритим ключем. Однонапрямлені функції.	**2**	2						Ознайомитися з поняттям асиметричних криптосистем.			
Однонапрямлені функції.	**2**	2						Знати про однонапрямлені функції.			
Вітчизняний стандарт шифрування даних. Режим простої заміни. Режим гамування. Режим гамування зі зворотним зв'язком. Режим вироблення імітовставки.	**2**					2		Знати про вітчизняний стандарт шифрування даних, режим простої заміни, режим гамування, режим гамування зі зворотним зв'язком, режим вироблення імітовставки.			
Режим гамування із зворотним зв'язком	**2**					2		Знати про режим гамування із зворотним зв'язком,			

Назви змістових модулів і тем	Кількість годин денна форма у тому числі						Аудіовізуальне, комп'ютерне та інше оснащення занять	Основні знання і вміння за темою	Домашнє завдання	Перелік літератури	Календарні строки проведення занять
	усього	лекції	практичні	лабораторні	семінарські	самостійна робота					
Криптосистема з депонуванням ключа. Загальні відомості. Процедура генерації ключів.	**2**					2		криптосистему з депонуванням ключа, загальні відомості, процедури генерації ключів.			
П.р.№5 Криптосистема Віжинера.	**2**	2						Ознайомитися з алгоритмом шифрування Віжинера.			
Криптосистема шифрування даних RSA.	**2**	2						Ознайомитися з алгоритмом шифрування та дешифрування RSA.			
Криптосистема шифрування даних RSA.	**2**	2						Ознайомитися з алгоритмом шифрування та дешифрування RSA.			
Алгоритм RSA.	**2**					2		Ознайомитися з алгоритмом шифрування RSA.			
П.р.№6 Алгоритм RSA.	**2**		2					Ознайомитися з алгоритмом шифрування RSA.			
П.р.№6 Алгоритм RSA.	**2**		2					Ознайомитися з алгоритмом шифрування RSA.			
Засоби керування системою.	**2**	2						Ознайомитися системою захисту інформації			
Погрози безпеки.	**2**	2						Ознайомитися із поняттям безпеки та основними погрозами.			
Шкідливе програмне забезпечення.	**2**	2						Ознайомитися із поняттям та типами шкідливого програмного забезпечення			

Назви змістових модулів і тем	Кількість годин денна форма у тому числі						Аудіовізуальне, комп'ютерне та інше оснащення занять	Основні знання і вміння за темою	Домашнє завдання	Перелік літератури	Календарні строки проведення занять
	усього	лекції	практичні	лабораторні	семінарські	самостійна робота					
Комп'ютерні віруси та їх властивості. Основні види вірусів та схеми їх функціонування.	**2**					2		Ознайомитися із поняттям комп'ютерних вірусів, їх ознаками та властивостями			
Підвиди хробаків та троянських програм.	**2**	2						Ознайомитися з підвида хробаків, троянських програм, схемами функціонування			
Шляхи проникнення вірусів у ПК. Програми виявлення вірусів.	**2**	2						Ознайомитися зі шляхами проникнення вірусів на носії даних та персональні комп'ютери.			
Компю'терні злочини та засоби захисту інформації у законодавстві.	**2**	2						Ознайомитися з поняттям комп'ютерних злочинів та засобами захисту інформації від них, які надає законодавство України			
Разом за змістовим модулем 2.1	**78**	**32**	**14**	**--**	**--**	**32**					
Всього годин за семестр	**90**	**38**	**14**	**--**	**--**	**38**					