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

ЗАТВЕРДЖУЮ
Директор ФКПАІТ ОНТУ
_____Ольга ЄПУР
___._____.2022 року

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ
(назва навчальної дисципліни)

ПРОГРАМА
нормативної навчальної дисципліни

підготовки_____фахового_молодшого бакалавра_____
(назва освітньо-кваліфікаційного рівня)

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

РОЗРОБЛЕНО ТА ВНЕСЕНО: Фаховий коледж промислової автоматики та інформаційних технологій Одеського національного технологічного університету

(повне найменування вищого навчального закладу)

УКЛАДАЧ ПРОГРАМИ: викладач вищої категорії Фахового коледжу промислової автоматики та інформаційних технологій ОНТУ Юлія БУРМАКІНА

Обговорено та рекомендовано до видання цикловою комісією «Комп'ютерних наук та інженерії програмного забезпечення» ФКПАІТ ОНТУ

___._____.2022 року, протокол №_____

Вступ: Програма вивчення нормативної навчальної дисципліни «Технології захисту інформації» складена відповідно до освітньо-професійної програми підготовки фахового молодшого бакалавра спеціальності 122 «Комп'ютерні науки».

Предметом вивчення навчальної дисципліни є моделі, методи, засоби та інформаційні технології захисту інформації в інформаційно-телекомунікаційних системах; алгоритми шифрування інформації; різновиди криптографічних систем.

Міждисциплінарні зв'язки: Пропонований курс ґрунтується на знаннях, отриманих студентами при вивченні таких дисциплін, як "Інформатика", "Архітектура комп'ютерів", "Організація баз даних та знань", "Технологія створення програмних продуктів", "Об'єктно-орієнтоване програмування". Вивчення курсу є базою для наступного опанування таких дисциплін: "Тестування програмних систем і комплексів", " Адміністрування програмних систем і комплексів ".

1 Мета та завдання навчальної дисципліни

1.1 Метою вивчення навчальної дисципліни є оволодіння студентами теоретичних знань та набуття практичних навиків з дисципліни «Технології захисту інформації», необхідних для спеціальної підготовки та майбутньої професійної діяльності.

1.2 Основна задача навчальної дисципліни «Технології захисту інформації» полягає у формуванні у студентів на основі системного підходу певного світогляду, який дозволяє їм вільно орієнтуватись в усьому різноманітті сучасних криптографічних алгоритмів та методів захисту інформації, основ вірусології, сформувати уявлення про комп'ютерні віруси, середовище їх існування та поширення, а також опанувати сучасні антивірусні програми та системи. для цього необхідні знання структурних особливостей конкретних систем, принципів їх побудови та алгоритмічного забезпечення, властивостей та характеристик, а також уміння застосовувати сучасні технічні засоби.

1.3 Згідно з вимогами освітньо-професійної програми студенти повинні:

Знати:

- Загальні поняття захисту інформації та інформаційної безпеки, джерела і способи дії загроз на об'єкти інформаційної безпеки установ, про правові і нормативні акти, які визначають систему захисту інформації в державі;

- Класичні та сучасні криптографічні системи захисту інформації та вміти застосовувати вивчені криптографічні алгоритми на практиці;
- Загальні поняття вірусології, погрози безпеки, основні типи та види комп'ютерних вірусів, принципи функціонування, методи їх проникнення у системи збереження даних та методи захисту комп'ютерів від вірусів.

Вміти:

- Використовувати практичні навички організації захисту інформації у системах збереження даних;
- На практиці реалізувати захист інформації з використанням симетричних, асиметричних криптографічних систем та електронного цифрового підпису;
- Оцінити переваги та недоліки різних криптографічних методів захисту інформації.
- Вміти працювати з базовими програмними методами захисту інформації при роботі з комп'ютерними системами та організаційними заходами і прийомами антивірусного захисту.
- Вміти проектувати систему захисту інформації.
- Вміти забезпечувати інформаційну безпеку за допомогою засобів, які здійснюють розгалуження доступу до інформації в автоматизованих системах.
- Вміти використовувати методи, засоби та стандарти захисту програмних систем та даних в умовах супроводу та експлуатації програмних систем і комплексів
- Вміти оцінювати програмне забезпечення і перспективи його використання з урахуванням професійних завдань, що вирішуються.

Володіти такими компетенціями:

- *загальнонаукові* – розуміння причинно-наслідкових зв'язків, володіння базовими поняттями та методами захисту інформації, базові знання сучасних технологій захисту інформації;

- *інструментальні* – навички роботи з комп’ютером, дослідницькі навички;
- *загально-професійні* – здатність застосовувати та створювати компоненти багаторазового застосування;
- *спеціально-професійні* – здатність застосовувати професійно-профільовані знання й уміння в галузі практичного використання комп’ютерних технологій з метою адміністрування (обслуговування, експлуатації та вдосконалення) програмних систем і комплексів для реалізації процесів захисту інформації та подальшого її ефективного використання.

На вивчення навчальної дисципліни відводиться **90** годин / **3** кредити ECTS.

2. Інформаційний обсяг навчальної дисципліни

2.1 Тематичний план

№ з/п	Назва розділів, тем програм, зміст занять	Всього годин	Кількість годин			
			У тому числі			
			Лекції	Лабораторні	Практичні	Самостійні
1	2	3	4	5	6	7
1	**Блок змістових модулів 1. Основні положення**					
1.1	Поняття інформаційної безпеки.	2	2			
1.2	Основні поняття і положення захисту інформації в комп’ютерних системах. Об’єкти захисту інформації	2	2			
1.3	Принципи криптографічного захисту. Класифікація методів криптографічного перетворення інформації.	2	2			
2	**Блок змістових модулів 2. Методи і засоби захисту інформації в комп'ютерних системах**					
2.1	Симетричні криптосистеми. Шифри перестановки. Шифр Сцитала. Шифруючі	8	2			6

	таблиці. Шифр маршрутної перестановки. Шифр поодинокої перестановки по ключу.					
2.2	Метод шифрування подвійною перестановкою	2	2			
2.3	П.р.№1 Шифри перестановки. Маршрутна перестановка та перестановка по ключу. Метод шифрування подвійною перестановкою	2			2	
2.4	Шифри заміни. Шифр Цезаря. Афінна система підстановок Цезаря. Мультиплікативна інверсія. Розширений алгоритм Евкліда. Система Цезаря з ключовим словом.	8	2			6
2.5	П.р.№2 Шифри заміни. Шифр Цезаря. Афінна система підстановок Цезаря.	2			2	
2.6	П.р.№3 Система Цезаря з ключовим словом	2			2	
2.7	Шифр Полібія. Шифруючі таблиці Трисемуса.	6	2			4
2.8	П.р.№4 Шифр Полібія. Шифруючі таблиці Трисемуса.	2			2	
2.9	Багатоалфавітні шифри. Шифр Хасегаві.	8	2			6
2.10	Асиметричні криптосистеми. Концепція криптосистеми з	8	2			6

	відкритим ключем. Однонапрямлені функції.					
2.11	Криптосистема Віжинера.	2	2			
2.12	П.р.№5 Криптосистема Віжинера.	2			2	
2.13	Криптосистема шифрування даних RSA.	4	4			
2.14	П.р.№6 Алгоритм RSA.	10			4	6
2.15	Засоби керування системою.	2	2			
2.16	Погрози безпеки.	2	2			
2.17	Шкідливе програмне забезпечення.	2	2			
2.18	Комп'ютерні віруси та їх властивості. Основні види вірусів та схеми їх функціонування.	6	2			4
2.19	Підвиди хробаків та троянських програм.	2	2			
2.20	Шляхи проникнення вірусів у ПК. Програми виявлення вірусів.	2	2			
2.21	Компю'терні злочини та засоби захисту інформації у законодавстві.	2	2			
	Всього за семестр	**90**	**38**		**14**	**38**

2.2 Програма навчальної дисципліни

Блок змістових модулів №1: Основні положення

Тема, зміст навчального матеріалу	Вимоги до загальноосвітньої підготовки студентів
Основні положення. Інформаційна безпека. Завдання захисту користувальницької інформації. **Криптографія. Класичні системи криптографії.** Основні поняття та термінологія у криптографії. Вимоги до криптографічних систем. **Історичний огляд криптографії.** Шляхи виникнення перших криптографічних алгоритмів. Простіші криптографічні алгоритми, їх розвиток. **Сучасні методи захисту інформації.** Сучасні криптографічні системи. Характеристика та види сучасних систем захисту інформації. **Асиметричні криптосистеми.** Загальне поняття та характеристики асиметричних криптосистем.	Студенти: *знають* основні поняття та визначення інформаційної безпеки, моделі систем, поняття та завдання захисту інформації користувача; *розуміють* поняття, термінологію та основні принципи криптографії та криптографічних систем; вимоги та характеристики стандарту криптографічних систем; шляхи виникнення перших криптографічних алгоритмів; *розрізняють* простіші криптографічні алгоритми, їх характеристики та ефективність, етапи розвитку криптографічних моделей; *здатні* опанувати основні поняття, сучасні методи криптографії, види сучасних систем захисту інформації та їх характеристики;

Блок змістових модулів №2: Методи і засоби захисту інформації в комп'ютерних системах

Тема, зміст навчального матеріалу	Вимоги до загальноосвітньої підготовки студентів
Симетричні криптосистеми. Алгоритм роботи симетричних криптосистем. **Криптосистема Цезаря.** Основні особливості криптосистеми Цезаря.	Студенти: *знають* основні поняття та визначення симетричних криптосистем, їх алгоритми роботи та ефективність; історію створення, особливості роботи та алгоритми

Генерація псевдо-випадкових ключів заміни. Алгоритми криптоперетворень. Ефективність методу. **Загальні поняття асиметричних криптосистем.** Алгоритм роботи асиметричних криптосистем. **Криптосистема RSA.** Алгоритм генерації відкритого та таємного ключів. Алгоритми криптоперетворень. Ефективність методу. **Багатоалфавітні системи.** Алгоритм Алгоритми крипто-перетворень. Ефективність методу. **Стандарти на основі принципу асиметричних криптосистем. Система Ель-Гамаля.** Основні особливості криптосистем. Алгоритми криптоперетворень.	криптоперетворення симетричної системи *знають* основні поняття та визначення асиметричних криптосистем, їх алгоритми роботи та ефективність; історію створення, особливості роботи та алгоритми криптоперетворення асиметричної системи RSA, поняття генерації псевдо-випадкових ключів; основні поняття багатоалфавітних систем; *розуміють* поняття асиметричних криптосистем, поняття стандартів на основі принципу асиметричних криптосистем, принципи їх роботи; алгоритм криптосистеми RSA, генерації відкритого та таємного ключів; поняття генерації квадрату *можуть* опанувати та знати поняття комп'ютерних злочинів, ключову термінологію та відповідальність за комп'ютерні злочини, що передбачено законодавством України.

3 Рекомендована література

3.1 Основна література

1. Ємець В., Мельник А., Попович Р. Сучасна криптографія. Основні поняття. – Львів: БАК, 2005 – 144 с.
2. Корольов Інформаційна безпека. – Харків :ХФН, 2000
3. Браіловський М.М., Хорошко В.О., Чирков Д.В., Чекет І.В. Основи захисту інформації. Навчальний посібник К.: НАУ, 2004. – 88 с.

3.2 Додаткова література

1. Коваленко М. М. Комп’ютерні віруси і захист інформації. — К.: Наук. думка, 2000. — 268 с.

2. Олецький О. В. Принципи роботи комп’ютерних систем: Навч. посіб. — К.: Вид. дім “КМ Академія”, 2003. — 144 с.

4 Критерії оцінювання навчальних досягнень студентів співвідносяться з рівнями компетентності з дисципліни і визначаються оцінками за виконання студентами практичних (лабораторних) робіт та рівня їх знань з окремих тем або групи послідовних тем за результатами підсумкового контролю.

- ТЕОРЕТИЧНИХ ЗНАНЬ СТУДЕНТІВ

«відмінно» заслуговує студент, який показав систематичне та глибоке знання питань матеріалу не тільки в обсязі лекцій, але й матеріалів, рекомендованих до самостійної роботи, а також додаткової літератури. При цьому студент повинен демонструвати вміння аналізувати інформацію, проявити творчі здібності у розумінні матеріалу.

«добре» отримає студент, який показав належне знання навчальної програми, виконав усі завдання, при цьому допустив незначні помилки та мав невеликі недоліки. При цьому студент показав систематичний характер знань з дисципліни, належний рівень знання рекомендованої літератури, самостійно робить висновки.

«задовільно» заслуговує студент, який показав знання основного матеріалу навчальної програми курсу у обсязі, необхідному для подальшого навчання та професійної діяльності, робить деякі помилки не принципового характеру.

«незадовільно» отримують студенти, які не змогли показати необхідний рівень знань для подальшого навчання, припустили значні помилки або зовсім не виконали програму курсу.

- ПРАКТИЧНИХ ВМІНЬ СТУДЕНТІВ

«відмінно» заслуговує студент, який виконав практичну роботу в повному об'ємі, і її виконання відповідає наступним вимогам:

- охоплює усі істотні аспекти завдання і контрольних питань;
- завдання роботи виконане студентом самостійно і на високому рівні;
- при виконанні роботи дотримані загальні зауваження і поради викладача;

- протокол практичної роботи оформлений акуратно, грамотно структурований, не містить довільних скорочень і інформації, що не відноситься до теми роботи;
- робота виконана і захищена своєчасно.

«добре» заслуговує студент, який виконав практичну роботу в повному об'ємі, і її виконання відповідає наступним вимогам:

- правильне розуміння студентом завдання і контрольних питань;
- завдання роботи виконане студентом самостійно, допущені незначні помилки, які так само були виправлені самостійно за порадами викладача;
- звіт роботи оформлений в цілому акуратно, але містить численні виправлення; містить досить детальний опис предмету завдання і контрольних питань, у ньому приведені і розкриті в тезовій формі основні поняття, відсутні помилкові положення;
- робота виконана і захищена своєчасно.

«задовільно» заслуговує студент, який виконав практичну роботу в повному об'ємі, і її виконання відповідає наступним вимогам:

- неповне або неточне виконання завдання і розкриття контрольних питань, а також окремих основних понять, що відносяться до практичної роботи;
- містить окремі помилкові положення, які, проте не роблять визначального впливу на виконання завдання;
- звіт оформлений неакуратно, містить виправлення об'ємних структурних частин і значну кількість нечітких формулювань.

«незадовільно» отримують студенти, які:

- не змогли показати необхідний рівень знань для виконання практичного завдання;
- припустили значні помилки: виконання завдання практичної роботи є неправильним в цілому і містить, в основному, помилкові положення; не розкриті основні поняття, що відносяться до предмета завдання практичної роботи;
- зовсім не виконали практичну роботу.

Переведення показників успішності знань студентів ФКПАІТ ОНТУ в систему оцінювання за шкалою ECTS

Оцінка за шкалою ECTS		Оцінка за бальною шкалою, що використовується в ФКПАІТ ОНТУ	Оцінка за національною шкалою	Оцінка за шкалою ОНТУ
відмінне виконання	A	12-11	Відмінно	100-93
вище середнього рівня	B	10		92-88
взагалі робота правильна, але з певною кількістю помилок	C	9-7	Добре	74-87
непогано, але зі значною кількістю недоліків	D	6	Задовільно	73-70
виконання задовольняє мінімальні критерії	E	5-4		60-69
потрібне повторне перескладання	FX	3	Незадовільно	40-59
повторне вивчення дисципліни	F	2-1		0-39

5 Форма підсумкового контролю успішності навчання: залік (VII семестр).

Оцінювання знань студента під час практичних занять та виконання індивідуальних завдань проводиться за 12-бальною або національною шкалою за такими критеріями:

1) ступінь засвоєння фактичного теоретичного матеріалу навчальної дисципліни;

2) ознайомлення з рекомендованою літературою, а також із сучасною літературою з питань, що розглядаються;

3) уміння поєднувати теорію з практикою при розв’язанні задач, проведенні розрахунків при виконанні індивідуальних завдань, та завдань, винесених на розгляд в аудиторії;

4) якість розробки моделей системи;

5) логіка, структура, стиль викладу матеріалу в письмових роботах, звітах і при виступах в аудиторії, вміння обґрунтовувати свою позицію, здійснювати узагальнення інформації та робити висновки.

Оцінка "відмінно" (10 – 12 балів) ставиться за умови відповідності індивідуального завдання студента, або його усної відповіді усім п’ятьом зазначеним критеріям. Відсутність тієї або іншої складової знижує оцінку на відповідну кількість балів.

При оцінюванні індивідуальних завдань увага також приділяється якості, самостійності та своєчасності здачі виконаних завдань викладачу (згідно з графіком навчального процесу). Якщо якась із вимог не буде виконана, то оцінка, на розсуд викладача, буде знижена.

Проведення поточно-модульного контролю. Поточно-модульний контроль здійснюється два рази у рамках вивчення курсу та оцінюється за трьома складовими: практичний модульний контроль, теоретичний модульний контроль і модульний контроль виконання ІНДЗ.

Оцінка за практичну складову модульного контролю виставляється за результатами оцінювання знань студента під час захисту практичних робіт та проміжного тестового контролю згідно з графіком навчального процесу.

Теоретичний модульний контроль здійснюється у письмовій формі, у вигляді контрольних опитувань на кожному практичному занятті. Оцінка за теоретичну складову модульного контролю виставляється за результатами контрольних опитувань і поточних оцінок студента на практичних заняттях.

Оцінка за ІНДЗ виставляється за результатами оцінювання знань студента при захисті індивідуальних завдань і враховує своєчасність їх виконання. Для підведення підсумків роботи студентів в кінці семестру виставляється підсумкова оцінка (оцінка за ККР).

6 Засоби і методи діагностики успішності навчання: тести, письмові самостійні роботи, усні опитування, контрольні завдання, захист звітів з практичних робіт, проведення поточно-модульного контролю.