Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних наук та інформаційних технологій (№ 302)

ЗАТВЕРДЖУЮ

Гарант освітньої програми

_____ О.Є. Федорович
(підпис) (ініціали та прізвище)

«____» _____ 2021 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології захисту інформації

(назва навчальної дисципліни)

Галузь знань: 12 «Інформаційні технології»
(шифр і найменування галузі знань)

Спеціальність: 122 «Комп'ютерні науки»
(код і найменування спеціальності)

Освітня програма: «Комп'ютеризація обробки інформації та управління»
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2021 рік

Розробник: Губка О.С., доцент, к.т.н., доцент
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп'ютерних наук та інформаційних технологій

Протокол № 634/08 від «30» серпня 2021 р.

Завідувач кафедри _ д.т.н., професор _____ О.Є. Федорович
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показника</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни (денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 6</td><td rowspan="11">Галузь знань
12 «Інформаційні технології»
(шифр та найменування)

Спеціальності:
122 «Комп’ютерні науки»

Освітні програми:
«Комп’ютеризація обробки інформації та управління»

Рівень вищої освіти:

перший (бакалаврський)</td><td>Цикл професійної підготовки</td></tr>
<tr><td>Кількість модулів – 2</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 2</td><td>2021/ 2022</td></tr>
<tr><td>Індивідуальне завдання: РР «Криптографічні методи захисту інформації».</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 60/180</td><td>8-й</td></tr>
<tr><td>Лекції</td></tr>
<tr><td rowspan="7">Кількість тижневих годин для денної форми навчання: аудиторних – 5 , самостійної роботи студента – 7</td><td>36 годин</td></tr>
<tr><td>Практичні, семінарські</td></tr>
<tr><td>–</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>24 години</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>120 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить:
для денної форми навчання – 60/120

[1)] Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета: надати студентам знань з методів та засобів забезпечення інформаційної безпеки, захисту інформаційних ресурсів та об’єктів критичної інфраструктури.

Завдання: вивчити основні методології захисту інформації для створення надійних комп'ютерних систем.

Фахові компетентності спеціальності (ФК):

– 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 (ФК7);

– здатність забезпечити організацію обчислювальних процесів в інформаційних системах різного призначення з урахуванням архітектури, конфігурування, показників результативності функціонування операційних систем і системного програмного забезпечення (ФК11);

– здатність до обґрунтованого вибору методів та технологій побудови Web-додатків та Web-сайтів з урахуванням можливостей пошукових систем мережі, а також їх адаптації з використанням механізму та алгоритмів роботи пошукових систем (ФК14);

Програмні результати навчання:

– демонструвати знання концепції інформаційної безпеки, принципів безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних (ПРН13);

– виконувати паралельні та розподілені обчислення, застосовувати чисельні методи та алгоритми для паралельних структур, мови паралельного програмування при розробці та експлуатації паралельного та розподіленого програмного забезпечення (ПРН14).

У результаті вивчення даної дисципліни студент повинен знати:

- місце і роль захисту інформації у програмному забезпеченні ІУС;
- структуру, принципи організації та функціонування сучасних систем захисту інформації;
- симетричні та асиметричні алгоритми шифрування;

На підставі отриманих теоретичних знань студент повинен уміти:

- використовувати принципи захисту інформації при проектуванні ІУС;

застосовувати сучасні алгоритми шифрування у захисті даних в ІУС;

будувати модель загроз технологічної безпеки;

Крім того студент повинен мати уявлення:

- про інструменти захисту інформації;
- історію розвитку криптографії;
- класифікацію вірусів.

Міждисциплінарні зв'язки: дисципліна «Технології захисту інформації» базується на наступних дисциплінах, які були вивчені студентами на попередніх курсах:

- «Проектування інформаційних систем»;
- «Технологія створення програмних продуктів».

Дана дисципліна зв'язана з наступними дисциплінами, які вивчаються студентами пізніше:

- «Розподілені системи обробки інформації та управління»;
- «Системне проектування»;
- «Системний аналіз» (КР).

3. Програма навчальної дисципліни

Модуль 1.

Змістовий модуль 1.

Тема 1. Вступ до навчальної дисципліни «Технології захисту інформації».

Предмет, об'єкт, мета і задачі вивчення дисципліни. Місце і роль курсу в системі дисциплін з напрямку 6.050101. Основні тенденції розвитку методів захисту ПК і криптографічних систем. Історія розвитку криптографії.

Тема 2. Класифікація небезпек для ПЗ ІС.

Визначення програмного забезпечення ІС. Класифікація ПЗ. Вимоги до ПЗ. Антивірусний захист ПК. Фізичний захист ПК. Антишпигунський захист ПК. Криптографічний захист даних ПЗ ІУС. Авторизация доступу в операційних системах (FreeBSD, MacOS X, Linux).

Тема 3. Загальні поняття криптографічного захисту інформації.

Поняття шифру. Оцінка якості шифрів. Різновиди задач криптографічного аналізу. Абсолютна стійкість та стійкість у операціях. Термінологія з захисту інформації.

Тема 4. Системи відкритого шифрування.

Синтез якісних шифрів. Системи відкритого розподілення ключів та системи відкритого шифрування. Системи Диффи-Хеллмана и RSA. Алгоритми шифрування DSA, MD4, MD5. Аналіз криптографічної стійкості алгоритмів шифрування. Електронний цифровий підпис та печатка (ЕЦП).

Компоненти ЕЦП. Поняття та свойства хеш-функції. Протокол ЕЦП Ель-Гамаля.

Тема 5. Загальні відомості про ГОСТ 28147-89 (ДСТУ ГОСТ 28147:2009).

Реалізація алгоритму ГОСТ. Базові цикли криптографічних перетворень. Базові режими шифрування. Оптимізація ГОСТ на мові високого рівня.

Тема 6. Антивірусний захист даних.

Методи боротьби з комп'ютерними вірусами. Класифікація комп'ютерних вірусів. Віруси-трояни. Віруси-черв'яки. Програми-монітори. Програми-сканери.

Модульний контроль.

Модуль 2.

Змістовий модуль 2.

Тема 7. Алгоритми генерації випадкових чисел.

Поняття програмного датчику випадкових чисел (ПДВЧ). Модель функціонування ПДВЧ. Вибір алгоритму ПДВЧ. Вибір алгоритму ПДВЧ.

Тема 8. Криптографічні інтерфейси.

Термінологія. Поняття зовнішнього сервісу безпеки. Огляд функцій інтерфейсу CryptoAPI. Системні питання реалізації засобів криптографічного захисту інформації (ЗКЗІ). Засоби та особливості реалізації криптографічних систем. Криптографічний захист транспортного рівня. Криптографічний захист прикладного рівня.

Тема 9. Забезпечення надійності криптографічних алгоритмів.

Основні підходи забезпечення відмовостійкості. Специфічні питання забезпечення надійності програмної реалізації криптографічних алгоритмів захисту даних. Методологія побудови надійних ЗКЗІ.

Тема 10. Особливості криптографічних засобів (КЗ).

Ліцензування КЗ. Сертифікація КЗ. Стандартизація КЗ. Законодавча база України стосовно захисту інформації.

Тема 11. Заключна лекція.

Перспективи розвитку технологій захисту інформації.

Модульний контроль.

Індивідуальне завдання – виконання РР на тематику «Криптографічні методи захисту інформації».

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	денна форма				
	усього	у тому числі			
		л	п	лаб	с.р.
Модуль 1					
Змістовий модуль 1.					
Тема 1. Вступ до навчальної дисципліни «Технології захисту інформації».	12	4	-	-	8
Тема 2. Класифікація небезпек для ПЗ ІС.	12	4	-	-	8
Тема 3. Загальні поняття криптографічного захисту інформації.	16	4	-	4	8
Тема 4. Системи відкритого шифрування.	16	4	-	4	8
Тема 5. Загальні відомості про ГОСТ 28147-89 (ДСТУ ГОСТ 28147:2009).	16	4	-	4	8
Тема 6. Антивірусний захист даних.	13	4	-	4	5
Усього годин	**85**	**24**	**-**	**16**	**45**
Модуль 2					
Змістовий модуль 2.					
Тема 7. Алгоритми генерації випадкових чисел.	19	2	-	2	15

Назви змістових модулів і тем	Кількість годин				
	денна форма				
	усього	у тому числі			
		л	п	лаб	с.р.
Тема 8. Криптографічні інтерфейси.	19	2	-	2	15
Тема 9. Забезпечення надійності криптографічних алгоритмів.	21	2	-	4	15
Тема 10. Особливості криптографічних засобів	12	2	-	-	10
Тема 11. Заключна лекція.	4	4	-	-	-
Усього годин	**75**	**12**	**-**	**8**	**55**
Індивідуальне завдання	20				20
Усього	**180**	**36**	**-**	**24**	**120**

5. Теми семінарських занять.

№ з/п	Назва теми	Кількість годин
1	Не передбачено навчальним планом	

6. Теми практичних занять.

№ з/п	Назва теми	Кількість годин
1	Не передбачено навчальним планом	

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Електронні ключі для захисту інформаціїї (eToken).	4
2	Антивірусні та антишпигунські програми та пакети (AVP Kaspersky, Avira Antivir Personal, NOD 32).	4
3	Електронний цифровий підпис та печатка.	4
4	Симетричний алгоритм шифрування ГОСТ 28147-89 (ДСТУ ГОСТ 28147:2009)	4
5	Шифруючи файлова система EFS (Windows 10).	4
6	Захист інформації у операційній системі Windows. Протокол Kerberos.	2
7	Асиметричний алгоритм шифрування RSA	2
	Разом	24

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Історія розвитку криптографії.	8
2	Фізичний захист ПК. Термінологія з захисту інформації.	8
3	Алгоритми шифрування DSA, MD4, MD5. Аналіз криптографічної стійкості алгоритмів шифрування. Протокол ЕЦП Ель-Гамаля.	8
4	Оптимізація ГОСТ на мові високого рівня.	8
5	Локальна аутентифікація користувача у операційній системі Windows.	8
6	Класифікація комп'ютерних вірусів.	8
7	Вибір алгоритму ПДВЧ.	8
8	Огляд функцій інтерфейсу CryptoAPI.	14
9	Криптографічний захист прикладного рівня.	15
10	Методологія побудови надійних ЗКЗІ.	15
11	Індивідуальне завдання	20
	Разом	120

9. Індивідуальні завдання

Виконання РР на тематику «Криптографічні методи захисту інформації».

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, індивідуальні консультації (при необхідності), самостійна робота студентів за матеріалами, опублікованими кафедрою (методичні посібники) та іншими матеріалами, в тому числі електронними.

11. Методи контролю

Проведення поточного контролю, контроль лабораторних робіт, модульний контроль, іспит.

12. Критерії оцінювання та розподіл балів, які отримують студенти

12.1. Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття	Кількість занять	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…1	8	0…8
Виконання і захист лабораторних робіт	0...5	4	0...20
Модульний контроль	0…12	1	0…12

Змістовний модуль 2			
Робота на лекціях	0…1	8	0…8
Виконання і захист лабораторних робіт	0...5	4	0...20
Модульний контроль	0…12	1	0…12
Виконання і захист РР	0…20		0…20
Усього за семестр			**0…100**

Семестровий контроль (іспит) проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається з 3 теоретичних запитань. За повну правильну відповідь на два перших запитання студент отримує по 33 бали. За повну правильну відповідь на останнє запитання –34 бали.

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки:

- місце і роль захисту інформації у програмному забезпеченні ІУС;
- структуру, принципи організації та функціонування сучасних систем захисту інформації;
- симетричні та асиметричні алгоритми шифрування;
- про інструменти захисту інформації;
- історію розвитку криптографії;
- класифікацію вірусів.

Необхідний обсяг вмінь для одержання позитивної оцінки:

- використовувати принципи захисту інформації при проектуванні ІУС;
- застосовувати сучасні алгоритми шифрування у захисті даних в ІУС;
- будувати модель загроз технологічної безпеки;

12.3 Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Мати мінімум знань та умінь. Відпрацювати та захистити всі лабораторні роботи та домашні завдання (РР). Вміти самостійно давати характеристику та описувати засоби захисту інформації. Знати класифікацію вірусів. Виявляти в структурі ПЗ програмні закладки.

Добре (75-89). Твердо мати мінімум знань, виконати усі завдання. Показати вміння виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з обґрунтуванням рішень та заходів, які запропоновано у роботах. Вміти використовувати принципи захисту інформації при проектуванні ІУС. Застосовувати сучасні алгоритми шифрування у захисті даних в ІУС.

Відмінно (90-100). Повно знати основний та додатковий матеріал. Знати усі теми. Орієнтуватися у підручниках та посібниках. Вміти використовувати

принципи захисту інформації при проектуванні ІУС. Застосовувати сучасні алгоритми шифрування у захисті даних в ІУС. Будувати модель загроз технологічної безпеки. Безпомилково виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з докладним обґрунтуванням рішень та заходів, які запропоновано у роботах.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

Горбенко І.Д., Гріненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації – Харків: ХНУРЕ, 2004. – 368 с.

14. Рекомендована література

Базова

1. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. - СПб.: Питер, 2012. – 544 с.
2. Казарин О.В. Безопасность программного обеспечения компьютерных систем. Монографія. – М.: МГУЛ, 2005. – 212 с.
3. Домашев А.В. Программирование алгоритмов защиты информации. – М.: «Нолидж», 2000. – 288 с.
4. Таненбаум Э. Современные операционные системы. – СПб.: Питер, 2012. – 1120 с.

Допоміжна

1. Шеннон К.Э. Теория связи в секретных системах. В кн. Работы по теории информации и кибернетике. М.: ИЛ, 1963. – 654 с.
2. Барсуков В.С., Водолазкий В.В. Современные технологии безопастности. – М.: «Нолидж», 2001. – 453 с.

15. Інформаційні ресурси

Сайт науково-технічної бібліотеки університету library.khai.edu