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

Кафедра комп'ютерних систем, мереж і кібербезпеки (№503)

ЗАТВЕРДЖУЮ

Керівник (гарант) освітньої програми

_____ А. В. Шостак
(підпис) (ініціали та прізвище)

« 30 » серпня 2024 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в комп'ютерних системах
(назва навчальної дисципліни)

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

Спеціальність: 123 «Комп'ютерна інженерія»
(код та найменування спеціальності)

Освітня програма: «Системне програмування»
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2024 рік

Робоча програма «Захист інформації в комп'ютерних системах»
(назва дисципліни)

Розробник: Карпенко А.С., ст. викладач, д-р філософії
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 30 » 08 2024 р.

Завідувач кафедри д.т.н., професор В. С. Харченко
(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 – 4</td><td rowspan="14">Галузь знань
12 «Інформаційні технології»
(шифр і найменування)

Спеціальність
123 «Комп’ютерна інженерія»
(код і найменування)

Освітня програма
«Системне програмування»
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 1</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів – 2</td><td>2024/2025</td></tr>
<tr><td rowspan="2">Індивідуальне завдання РР</td><td>Семестр</td></tr>
<tr><td>7-й</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 64/120</td><td>Лекції*</td></tr>
<tr><td>32 години</td></tr>
<tr><td rowspan="8">Кількість тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи студента – 3,5</td><td>Практичні, семінарські*</td></tr>
<tr><td>0 - годин</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>32 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>56 години</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 – 64/56.

*Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: ознайомлення тих, хто навчається, з методологією, основними напрямами, методами і алгоритмами реалізації функцій захисту інформації в комп'ютерних системах та мережах, а також придбанні навичок розрахунку параметрів сучасних криптографічних алгоритмів забезпечення захисту інформації, використанню стеганографічних методів захисту інформації та методам антивірусного захисту.

Завдання: вивчення принципів побудови криптографічних та стеганографічних алгоритмів забезпечення захисту інформації, антивірусного захисту, а також базових положень щодо реалізації комплексної системи захисту інформації в установі (підприємстві).

Компетентності, які набуваються:

- (ЗК1) здатність до абстрактного мислення, аналізу і синтезу;
- (ЗК2) здатність вчитися і оволодівати сучасними знаннями;
- (ЗК9) здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні;
- (ЗК10) здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя;
- (ФК1) здатність застосовувати законодавчу та нормативноправову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії;
- (ФК4) здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки;
- (ФК10) здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації;
- (ФК11) здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів;
- (ФК13) здатність вирішувати проблеми у галузі комп'ютерних та інформаційних технологій, визначати обмеження цих технологій;
- (ФК15) здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати та захищати прийняті рішення;
- (ФК17) здатність розробляти, налагоджувати та адмініструвати системи управління контентом (CMS) для веб-застосунків.

Очікувані результати навчання:

- (ПРН1) знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж;
- (ПРН4) знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному екологічному контексті;
- (ПРН7) вміти розв'язувати задачі аналізу та синтезу засобів, характерних для спеціальності;
- (ПРН8) вміти системно мислити та застосовувати творчі здібності до формування нових ідей;
- (ПРН9) вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.

Пререквізити – «Теорія інформації і кодування», «Комп'ютерні мережі».
Кореквізити – «Кваліфікаційна робота бакалавра».

3. Програма навчальної дисципліни

Модуль 1.

Змістовий модуль 1. *Криптографія*

Тема 1. ***Основи захисту інформації в комп'ютерних системах***

Основні визначення. Терминологія. Загрози інформаційної безпеки. Нормативно - правова база. Технічни засоби захисту інформації.

Тема 2.*Симетричні криптологічні системи*

Основні класи симетричних криптосистем. Шифри перестановки. Таблиці, що шифрують. Система омофонів. Біграмні шифри. Шифри складної заміни. Багатоалфавітний шифр. Система Віженера. Одноразовий блокнот.

Тема 3. ***Алгоритми симетричного шифрування***

Алгоритми блокового шифрування. Характеристика алгоритмів блокового шифрування. Мережа Фейстела. Режими блокового шифрування. Алгоритм блокового шифрування DES. Схема шифрування. Функції алгоритму DES. Алгоритмі формування ключів. Алгоритм ДСТУ ГОСТ 28147 2009. Схема шифрування. Функції алгоритму DES. Алгоритм AES. Схема шифрування. Функції алгоритму AES. Алгоритм ДСТУ 7624:2014. Схема шифрування. Функції алгоритму ДСТУ 7624:2014. Шифрування методом гамування. Процес гамування. Конгруентний генератор. Генератор на регістрах зсуву. Побудова потокових шифрів.

Тема 4. ***Криптосистеми із відкритим ключем***

Теоретичні основи побудови криптосистем із відкритим ключем. Концепція криптосистем із відкритим ключем. Односпрямовані функції.

Криптосистема RSA. Криптосистема Ель Гамаля. Криптосистеми на еліптичних кривих.

Тема 5. ***Автентифікація та цифровий підпис***

Задача автентифікації. Задача автентифікації даних. Контроль незмінності масивів даних. Виробітку коду виявлення маніпуляцій. Цифровий підпис. Цифровий підпис на основі традиційних блокових шифрів. Цифрові підписи, засновані на асиметричних криптосистемах. Функція хешування. Багатоадресна автентіфікація. Багатоадресна автентіфікація без забезпечення невідмовлення. Багатоадресна автентіфікація з забезпеченням невідмовлення. Обмін ключами.

Модульний контроль

Змістовий модуль 2. ***Системи захисту інформації***

Тема 6 ***Антивірусний захист***

Загальна характеристика та класифікація комп'ютерних вірусів. Фізична структура комп'ютерного вірусу. Зараження програми. Файловий транзитний вірус. Бутовий вірус. Stealth-вірус. Поліморфні віруси. Макровіруси. Мережеві віруси. Характеристика засобів нейтралізації комп'ютерних вірусів. Антивіруси. Детектори. Фаги. Вакцини. Щеплення. Ревізори. Монітори. Методів захисту від комп'ютерних вірусів. Архівування. Вхідний контроль. Профілактика. Ревізія. Карантин. Сегментація. Фільтрація. Вакцинація. Автоконтроль цілісності. Терапія. Інтегрований програмний комплекс. Каталог детекторів. Програма-пастка вірусів. Програма для вакцинації. База даних про віруси і їх характеристиках. Резидентні засоби захисту. Технології виявлення шкідливого коду. Модель системи захисту від шкідливих програм. Технічний компонент. Аналітичний компонент. Антивірусні програми. Класифікація.

Тема 7. ***Стеганографія***

Узагальнена модель стегосистеми. Вимоги. Основні програми стеганографії. Приховування даних (повідомлень). Цифрові водяні знаки. Заголовки. Області застосування стеганографії. Схема стегосистеми. Стеганографія з відкритим ключем. Виявлення ЦВЗ з нульовим знанням. Стегоалгоритму вбудовування. Інформації в зображення. Адитивні алгоритми. Алгоритми на основі лінійного вбудовування даних. Алгоритм боксу-Мюллера. Алгоритми на основі злиття ЦВЗ і контейнера. Стеганографічні методи на основі квантування. Принципи вбудовування інформації з використанням квантування. Дізерзованние Квантователь. Алгоритми вбудовування ЦВЗ з використанням скалярного квантування. Вбудовування ЦВЗ з використанням векторного квантування. Стегоалгоритму, що використовують фрактальное перетворення. Приховування даних в аудіосигнали. Методи кодування з розширенням спектра. Впровадження інформації модифікацією фази аудіосигналу. Вбудовування інформації за рахунок зміни часу затримки луна-сигналу. Методи маскування ЦВЗ. Приховування даних в відеопослідовність.

Стандарт mpeg і можливості. Впровадження даних. Методи вбудовування інформації на рівні коефіцієнтів

Модульний контроль

4. Структура навчальної дисципліни

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовий модуль 1. Криптографія					
Тема 1. Основи захисту інформації в комп'ютерних системах	6	4			2
Тема 2. Симетричні криптологічні системи	14	4		4	6
Тема 3. Алгоритми симетричного шифрування	14	4		4	6
Тема 4. Криптосистеми із відкритим ключем	14	4		4	6
Тема 5. Автентифікація та цифровий підпис	17	4		7	6
Модульний контроль	1			1	
Разом за змістовим модулем 1	66	20		20	26
Змістовний модуль 2. Системи захисту інформації					
Тема 6 Антивірусний захист	18	4		4	10
Тема 7. Стеганографія	29	8		7	14
Модульний контроль	1			1	
Разом за змістовим модулем 2	48	12		12	24
Разом за модулем 1	114	32		32	50
Модуль 2					
Індивідуальне завдання	6				6
Усього годин	**120**	**32**		**32**	**56**

5. Теми семінарських занять

№ п/п	Назва теми	Кількість годин
	Не передбачено.	
	Разом	

6. Теми практичних занять

№ п/п	Назва теми	Кількість годин

1	*Не передбачено.*	
	Разом	

7. Теми лабораторних занять

№ п/п	Назва теми	Кількість годин
1	Дослідження алгоритму багато абеткового шифру	4
2	Дослідження та порівняльний аналіз алгоритмів DES та AES	4
3	Дослідження алгоритму RSA	4
4	Дослідження алгоритму цифрового підпису	4
5	Дослідження алгоритму обміну ключами.	4
6	Дослідження можливості використання описаних вразливостей для вбудовування у вірусний код	4
7	Дослідження алгоритмів прихованої передачі інформації в текстовому файлі	4
8	Дослідження алгоритмів прихованої передачі інформації в нерухомому зображенні	4
	Разом	**32**

8. Самостійна робота

№ п/п	Назва теми	Кількість годин
1	Тема 1. Основи захисту інформації в комп'ютерних системах	2
2	Тема 2. Симетричні криптологічні системи	6
3	Тема 3. Алгоритми симетричного шифрування	6
4	Тема 4. Криптосистеми із відкритим ключем	6
5	Тема 5. Автентифікація та цифровий підпис	6
6	Тема 6 Антивірусний захист	10
7	Тема 7. Стеганографія	14
8	Розрахункова робота	6
	Разом	**56**

9. Індивідуальні завдання

№ з/п	Назва теми	*Кількість годин*
1	Розрахункова робота	6

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота здобувачів освіти за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного тестового контролю, тестового модульного контролю, підсумковий контроль у вигляді заліку.

12. Критерії оцінювання та розподіл балів, які отримують студенти

12.1. Розподіл балів, які отримують студенти (кількісні показники оцінювання) під час семестру

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Модуль 1 Змістовий модуль 1			
Робота на лекціях	0...1	10	0...10
Лабораторні заняття	0...5	5	0...25
Модульний контроль	0…24	1	0…12
Змістовий модуль 2			
Робота на лекціях	0...1	6	0...6
Лабораторні заняття	0...5	3	0...15
Модульний контроль	0…20	1	0…12
Модуль 2			
Розрахункова робота	0…20	1	0…20
Усього за семестр			**0…100**

12.2. Робота на лекції передбачає готовність та бажання студента висувати свої версії відповіді на поставлене питання, уміння та здатність відстоювати свою точку зору.

12.3. Оцінка за лабораторну роботу включає якість виконаної роботи, відповідність звіту виданому завданню, тимчасові обмеження (здавання звіту має відбутися протягом 2 тижнів з моменту проведення роботи)

12.4. Кожен модуль складається із 12 питань. На кожне запитання представляється 4 варіанти відповіді, з яких одна правильна. За кожну правильну відповідь ставиться 1.Час виконання – 25 хв.

12.5. Якщо під час семестру студент набирає менше 60 балів або не задоволений кількістю балів, які отримав під час семестру, то він має скласти семестровий іспит.

Білет для іспиту складається з двох теоретичних і одного практичного запитання. За теоретичні запитання студент отримує до 60 балів (до 30 балів за кожне) , за практичне – до 40 балів.

Під час складання семестрового іспиту здобувач має можливість отримати максимум 100 балів.

12.6 Таблиця переводу бальної системи оцінювання у традиційну

Сума балів	Оцінка за традиційною шкалою
	Іспит

90 – 100	Відмінно
75 – 89	Добре
60 – 74	Задовільно
0 – 59	Незадовільно

13. Методичне забезпечення

1. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=3737

2. Сторінка дисципліни у системі Classroom [Ел. ресурс]. URL: https://classroom.google.com/c/NjIwNjY2NjM1MTky?cjc=equsclq

14. Рекомендована література

Базова

1. Кузнецов О. О., Євсеєв С. П., Король О. Г. Стеганографія. Навчальний посібник. Харків: Вид. ХНЕУ, 2011. – 232 с.
2. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник / Запоріжжя : НУ «Запорізька політехніка», 2020. 192 с.
3. Дворецький М. Л., Нездолій Ю. О., Дворецька С. В., Кандиба І. О. Розробка мобільних застосунків для OS Android : навч. посіб. Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2021. 140 с.
4. Радченко К. О. Розроблення мобільних застосунків. Конспект лекцій : навч. пос., К.: КПІ ім. Ігоря Сікорського, 2021. 546 с.
5. Програмування мобільних пристроїв: навчальний посібник для дистанційного навчання / К.Т. Кузьма. – Миколаїв: СПД Румянцева Г. В., 2021. 128 с.
6. D. Griffiths, D. Griffiths. Head First Android Development: A Learner's Guide to Building Android Apps with Kotlin. O'Reilly Media, 2021. 913 p.
7. N. Metzler. Kotlin Programming for Beginners: An Introduction to Learn the Kotlin Programming Language with Tutorials and Hands-On Examples, Lightbulb Publishing, 2021. 162c.
8. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник.– К.: Видавництво НА СБ України, 2022. – 256 с.
9. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації: навчальний посібник. – Х.:Новий світ-2000, 2022. – 678 с

Допоміжна

1. A. Grant. Android for Absolute Beginners: Getting Started with Mobile Apps: Development Using the Android Java SDK, 2021. 204 p.
2. M. L. Murphy. Elements Of Android Room 0.5, Leanpub, 2021. 439 p.
3. J. DiMarzio Android Studio Game Development: Concepts and Design, 2021. 95c

15. Інформаційні ресурси

1.Тарнавський Ю. А. Технології захисту інформації URL: https://ela.kpi.ua/ bitstream/123456789/23896/1/TZI_book.pdf

2. Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних. URL: https://vfranchuk.fi.npu.edu.ua/ images/ files/ statty/32_ZIR_cript.pdf

3.Рейтинг найкращих антивірусів — ТОП-10 програм. https://itc.ua/ua/articles/reityng-antyvirusiv/