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

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

**ЗАТВЕРДЖУЮ**

Голова НМК 2

Д.М.Крицький
(підпис) (ініціали та прізвище)

«31» серпня 2022 р.

# РОБОЧА ПРОГРАМА ВИБІРКОВОЇ 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 і найменування спеціальності)

**Освітня програма:** Комп'ютерні системи та мережі

**Освітня програма:** Системне програмування
(найменування освітньої програми)

**Рівень вищої освіти**: перший (бакалаврський)

**Харків 2022 р.**

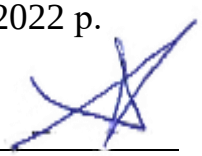
Розробник: Пєвнєв В.Я., доцент, д.т.н., доцент 

(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 .2022 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 – 4,5</td><td rowspan="11">Галузь знань<br>_12 "Інформаційні технології"<br>(шифр і найменування)<br><br>Спеціальність<br>123 "Комп’ютерна інженерія"<br>(код і найменування)<br><br>Освітня програма<br>Комп’ютерні системи та мережі<br>Системне програмування<br>(найменування)<br><br>Рівень вищої освіти:<br><br>перший (бакалаврський)</td><td>Вибіркова</td></tr>
<tr><td>Кількість модулів – 2</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів –2</td><td>2022/2023</td></tr>
<tr><td>Індивідуальне завдання - Розрахункова робота<br>(назва)</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 64/135</td><td>7-й</td></tr>
<tr><td>Лекції*</td></tr>
<tr><td rowspan="8">Кількість тижневих годин для денної форми навчання:<br>аудиторних – 4 год.<br>самостійної роботи студента – 4,5 год.</td><td>32 годин</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>32___годин</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>71 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить для денної форми навчання – 64/71.

[1)] 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.

**Завдання**: вивчення принципів побудови криптографічних алгоритмів забезпечення захисту інформації, а також базових положень щодо реалізації комплексної системи захисту інформації в установі (підприємстві), розуміти властивостіі інформаційних ресурсів та технологій, як об'єктів кібербезпеки, та вміння здійснювати класифікацію загроз безпеці інформаційних ресурсів, класифікацію та ранжирування джерел загроз і уразливостей безпеці, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; розуміти принципи і методи теорії захищених систем.

**Компетентності, які набуваються:**

- здатність до абстрактного мислення, аналізу і синтезу;
- здатність вчитися і оволодівати сучасними знаннями;
- здатність застосовувати знання у практичних ситуаціях;
- здатність спілкуватися державною мовою як усно, так і письмово;
- здатність спілкуватися іноземною мовою;
- навички міжособистісної взаємодії;
- вміння виявляти, ставити та вирішувати проблеми;
- здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки;
- здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

**Очікувані результати навчання:**

- знати новітні технології в галузі комп'ютерної інженерії;
- якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.

**Пререквізити**: дисципліна базується на знаннях, отриманих під час вивчення дисциплін із циклу загальної підготовки, зокрема "Організація баз даних", "Комп'ютерні системи", "Теорія електричних кіл і мікроелектроніка", " Дискретна математика ".

**Кореквізити** є підґрунтям для "Комп'ютерні мережі ", " Проектування вбудованих аерокосмічних систем ", для курсового та дипломного проектування.

## 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 Вижинера. 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. Криптоаналіз DES. Алгоритм ДСТУ. Схема шифрування. Функції алгоритму DES. Криптоаналіз DES. Шифрування методом гамування. Процес гамування. Генератори парних псевдовипадкових послідовностей. 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. Криптоаналіз систем із відкритим ключем. Класифікація алгоритмів факторизації. Алгоритм Полларда. Алгоритм Ленстра. Алгоритм факторизації на основі рішення нерівності Алгоритми генерації простих чисел. Модульний контроль.

### Модуль 2

Індивідуальне завдання

### Модуль 3

**Змістовний модуль 2.** ***Системи захисту інформації***

**Тема 5. Автентіфікация та цифровий підпис.**

Задача автентіфікації. Задача автентіфікації 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.

**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. Призначення програми AVZ і вирішуються нею завдання.

**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 | 9 | 4 | | | 5 |
| Тема 2. Симетричні криптологічні системи | 18 | 4 | | 4 | 10 |
| Тема 3. Алгоритми симетричного шифрування | 18 | 4 | | 4 | 10 |
| Тема 4. Криптосистеми із відкритим ключем. Модульний контроль | 22 | 4 | | 8 | 10 |
| Разом за змістовим модулем 1 | 67 | 16 | | 16 | 35 |
| **Модуль 2** | | | | | |
| Індивідуальне завдання | 6 | | | | 6 |
| **Модуль 3** | | | | | |
| **Змістовний модуль 2.** Системи захисту інформації | | | | | |
| Тема 5. Автентіфікация та цифровий підпис. Модульний контроль | 18 | 4 | | 4 | 10 |
| Тема 6 Антивірусний захист | 24 | 6 | | 8 | 10 |
| Тема 7. Стеганографія. Модульний контроль | 20 | 6 | | 4 | 10 |
| Разом за змістовим модулем 2 | 62 | 16 | | 16 | 30 |
| **Усього годин** | **135** | **32** | | **32** | **71** |

## 5. Теми семінарських занять

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | | |
| 2 | | |
| | **Разом** | |

## 6. Теми лабораторних занять

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | | |
| 2 | | |
| | **Разом** | |

## 7. Теми практичних занять

| № з/п | Назва теми | | Кількість годин |
|---|---|---|---|
| 1 | Алгоритми багато абеткового шифру | | 4 |
| 2 | Алгоритми блокового шифрування | | 4 |
| 3 | Алгоритм RSA | | 4 |
| 4 | Алгоритми криптоаналізу RSA | | 4 |
| 5 | Цифровий підпис на основі протоколу Шнора | | 4 |
| 6 | Виявлення вірусної активності вбудованими засобами ОС | | 4 |
| 7 | Можливості зараження ПК вірусним кодом | | 4 |
| 8 | Стеганографічні алгоритми | | 4 |
| | **Разом** | | 32 |

## 8. Самостійна робота

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | Тема 1. Основи захисту інформації в комп'ютерних системах | 5 |
| 2 | Тема 2. Симетричні криптологічні системи | 10 |
| 3 | Тема 3. Алгоритми симетричного шифрування | 14 |
| 4 | Тема 4. Криптосистеми із відкритим ключем | 10 |
| 5 | Тема 5. Автентіфікация та цифровий підпис | 10 |
| 6 | Тема 6 Антивірусний захист | 12 |
| 7 | Тема 7. Стеганографія | 10 |
| | **Разом** | 71 |

## 9. Індивідуальні завдання

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | Розрахункова робота по дослідженню симетричної системи шифрування | 6 |

## 10. Методи навчання

Проведення аудиторних лекцій, практичних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

## 11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

## 12. Критерії оцінювання та розподіл балів, які отримують студенти

| Складові навчальної роботи | Бали за одне заняття (завдання) | Кількість занять (завдань) | Сумарна кількість балів |
|---|---|---|---|
| **Модуль 1** | | | |
| Робота на лекціях | 0…1 | 8 | 0…8 |
| Виконання практичних робіт | 0...5 | 4 | 0...20 |
| Модульний контроль | 0…16 | 1 | 0…16 |
| **Модуль 2** | | | |
| Виконання і захист РР | 0…10 | 1 | 0…10 |
| **Модуль 3** | | | |
| Робота на лекціях | 0…1 | 8 | 0…8 |
| Виконання практичних робіт | 0...5 | 4 | 0...20 |
| Модульний контроль | 0…18 | 1 | 0…18 |
| **Усього за семестр** | | | **0…100** |

Контроль знань при проведенні занять оцінюється за такими шкалами:
активність на лекції під час відповідей на питання:
- активна робота на лекції - 1 бал;

виконання практичних робіт:
- при виконанні всіх вимог завдань методик на роботи - 5 бали;
- незначні недоліки при відповіді на питання при захисті результатів роботи за змістом досліджуваної теми - 4 бали;
- неповні відповіді на питання при захисті результатів роботи за змістом досліджуваної теми - 3 бали;
- неповні відповіді на питання за змістом і результатами роботи - 2 бала;
- недооформлені результати роботи і неповні відповіді на питання за змістом результатів роботи -1бал;
- якщо робота не виконана - 0 балів.

На модульний контроль виносяться всі пройдені за контрольований період теми, які включаються в варіанти завдань, що містять по 17 або 10 питаннь (по всім темам та видам занять). Максимальна кількість балів за кожне питання - 1.

Семестровий контроль у вигляді іспиту 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 двох теоретичних та одного практичного запитань, максимальна кількість за кожне із запитань, складає за теоретичними питаннями 30 балів, за практичнім - 40 балів.

## Критерії оцінювання роботи студента протягом семестру

**Задовільно (60-74).** Показати мінімум знань та умінь. Захистити не менше 80% від усіх завдань практичних занять. Уміти використовувати правові та нормативні документи, вітчизняних та міжнародних стандартів для проведення наукових робіт та робіт щодо забезпечення захисту інформації.

**Добре (75-89).** Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 90% завдань практичних занять. Уміти використовувати сучасні методи теоретичних та експериментальних досліджень для організації захисту інформації. Мати необхідний обсяг вмінь для одержання позитивної оцінки.

**Відмінно (90-100).** Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Уміти організувати й виконувати роботи з забезпечення захисту інформації..

**Шкала оцінювання: бальна і традиційна**

| Сума балів | Оцінка за традиційною шкалою |
|---|---|
| | Іспит |
| 90 – 100 | Відмінно |
| 75 – 89 | Добре |
| 60 – 74 | Задовільно |
| 0 – 59 | Незадовільно |

## 13. Методичне забезпечення

1. Тексти лекцій
2. Презентації лекцій
3. Керівництво до практичних робіт

## 14. Рекомендована література

**Базова**


1. Проскурин В. Г. Защита программ и данных: учеб. пособие М. : Издательский центр «Академия», 2012. 208 с.
2. Проскурин, В.Г. Защита в операционных системах [Электронный ресурс] : учеб. пособие для вузов. М. : Горячая линия – Телеком, 2014. 193 с.
3. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. 288 с.
4. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М.: Солон-Пресс, 2002. 272 с


**Допоміжна**


1. Столлингс В. Современные компьютерные сети. Спб.: Питер, 2003. 783 с.
2. Бирюков А.А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2012. 474 с.

3. Скляров Д. Искусство защиты и взлома информации. Спб.: БХВ-Петербург, 2004. 288 с.
4. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М.: Техносфера, 2006. 320 с.
5. Ачилов Р. Построение защищенных корпоративных сетей. М.: ДМК Пресс, 2013. 250 с.
6. Есин В.И., Кузнецов А.А., Сорока Л.С. Безопасность информационных систем и технологий. Х.: ООО «ЭДЭНА», 2010. : 656 с.
7. Разрушающие программные воздействия: Учебно-методическое пособие . под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2011. 328 с.

## 15. Інформаційні ресурси

1. http://www.solon-press/ ru
2. http://bookash.pro/ru/s/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B5+%D0%B2%D0%B8%D1%80%D1%83%D1%81%D1%8B/