МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

«**ЗАТВЕРДЖУЮ**»
Голова Вченої ради ЧДТУ
_____/_____
«_____» _____ 20___ р.

ПРОГРАМА
навчальної дисципліни

«КРИПТОГРАФІЧНІ МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ»

шифр (за ОПП) – ВФП9

підготовки здобувачів освітнього ступеня «бакалавр»

напряму підготовки – 6.170103 «Управління інформаційною безпекою»

2016 рік

РОЗРОБЛЕНО ТА ВНЕСЕНО КАФЕДРОЮ:
Інформаційної безпеки та комп’ютерної інженерії

Протокол засідання кафедри № __ від _____ 20 __ р.

РОЗРОБНИКИ ПРОГРАМИ: Стабецька Тетяна Анатоліївна, асистент кафедри інформаційної безпеки та комп'ютерної інженерії

Обговорено та рекомендовано до затвердження методичною комісією факультету інформаційних технологій і систем

«____» _____ 20___ р., протокол №__

ПОГОДЖЕНО

Навчально-методичний відділ _____ /_____/
підпис *ПІБ*

«____» _____20___ р.

ВСТУП

Програма навчальної дисципліни «Криптографічні методи та засоби захисту інформації» складена відповідно до освітньо-професійної програми підготовки здобувачів освітнього ступеня «бакалавр» напряму підготовки – *6.170103 «Управління інформаційною безпекою».*

Предметом вивчення навчальної дисципліни *«*Криптографічні методи та засоби захисту інформації*»* є забезпечення формування знань та вмінь, визначених освітньо-кваліфікаційною характеристикою, за сукупністю й рівнями їхньої сформованості, необхідними для вирішення професійних завдань.

Міждисциплінарні зв'язки: начальна дисципліна *«*Криптографічні методи та засоби захисту інформації*»* тісно пов'язана з такими дисциплінами, як «Вища математика», «Дискретна математика», «Теорія ймовірностей та математична статистика», «Теорія інформації та кодування», «Алгебра полів Галуа», «Комп'ютерна логіка», «Програмування та алгоритмічні мови», «Системне програмне забезпечення», «Основи криптографічного захисту інформації».

Мета викладання навчальної дисципліни полягає у формуванні у майбутніх фахівців сучасного рівня культури з інформаційної безпеки; набуття практичних навичок з основ застосування сучасних методів забезпечення криптографічного захисту інформації в комп'ютерних системах, формуванні у студентів розуміння основ інформаційної безпеки, вмінню застосовувати криптографічні методи шифрування, використовувати методи шифрування інформації для передачі у мережі, а також надання студентам системних знань з принципів побудови систем криптографічного захисту інформації в КС.

Завданнями вивчення навчальної дисципліни є:

- розгляд основних етапів історичного розвитку криптографії;
- оволодіння теоретичними знаннями про основні методи криптографічного захисту інформації;
- розгляд математичних моделей симетричних шифрів та їх властивостей;
- оволодіння основними способами шифрування даних;
- вивчення методів асиметричної криптографії;
- дослідження особливостей криптографічних алгоритмів та криптографічних протоколів;
- ознайомлення з основними положеннями нормативно-правового регулювання у галузі КЗІ;
- розгляд основних напрямків розвитку сучасних систем КЗІ.

Результати навчання: згідно з вимогами освітньо-професійної програми, після засвоєння навчальної дисципліни студенти мають продемонструвати такі результати навчання:

Знати:

- історію виникнення криптографії
- основні поняття криптографії;
- прості криптографічні методи захисту інформації, такі як афінний шифр Цезаря, шифр Віженера, шифр Вернама;
- основні криптографічні алгоритми симетричного шифрування;
- основні криптографічні алгоритми асиметричного шифрування та цифрового підпису.
- сучасні моделі криптографічних протоколів, таких як електроний цифровий підпис;
- методи аналізу стійкості криптографічних систем та засобів криптографічного захисту інформації;
- типові вимоги до систем та засобів управління ключовими даними;
- базові стандарти в галузі криптографічного захисту інформації.

Уміти:

- працювати з технічною літературою і документацією;
- використовувати сучасні криптографічні методи для захисту конфіденційної інформації;
- використовувати систему електронного підпису або режиму електронного цифрового підпису;
- застосовувати систему захисту інформації в автоматизованих системах;
- моделювати (проектувати) алгоритми криптографічних перетворень та елементи криптографічного аналізу на комп’ютері;

Досвід:

- обґрунтування та висування пропозицій щодо стандартних криптографічних систем, криптографічних примітивів та протоколів захисту ресурсів в КС та КМ;
- здійснення загальної оцінки якості криптографічного захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, що реалізовані з використанням засобів обчислювальної техніки.

На вивчення навчальної дисципліни відводиться 120 годин та 4 кредити ЄКТС.

1. Інформаційний обсяг навчальної дисципліни

Змістовий модуль 1. «Основні поняття криптографії. Криптографія з симетричним ключем»

Тема 1.1. *Базові поняття криптографії.*

Мета і задачі дисципліни. Основні поняття та визначення. Наука про шифрування. Роль криптографії у захисті даних.

Тема 1.2. *Історія кодування та шифрування. Використання кодів. Сучасна криптографія.*

Історія криптографії. Основні поняття криптографії та теорії секретних систем. Перші методи шифрування перестановки та заміни. Одноалфавітні системи шифрування Віженера, Плейфейра та інш. Багато алфавітні системи шифрування та їх роль у сучасній криптографії.

Тема 1.3. *Прості шифри перестановки. Криптоаналіз шифрів перестановки.*

Компоненти криптосистеми та їх функціональні характеристики. Перестановка та підстановка. Прості шифри. Криптоаналітичні атаки та метод підрахунку частот для моно та багатоалфавітних криптосистем.

Тема 1.4. *Шифри простої та складної заміни.*

Тема 1.5. *Багатоалфавітні шифри.*

Числові шифри. Книжкові шифри.

Тема 1.6. *Симетричні алгоритми.*

Блочні та поточні шифри. Принципи побудови, функціонування та криптоаналізу симетричних блокових алгоритмів шифрування DES (Digital Encryption Standard), ГОСТ 28147-89, AES.

Тема 1.7. *Шифрування із паролем.*

Апаратні пристрої збереження ключів. Криптографічні акселератори. Біометрична ідентифікація.

Змістовий модуль №2. «Розподіл ключів та криптографія з відкритим ключем»

Тема 2.1. *Розподіл ключів. Використання довіреної третьої сторони.*

Тема 2.2. *Криптографія з відкритим ключем та цифрові конверти.*

Алгоритм RSA. Алгоритм Діффі (DH). Алгоритм еліптичних кривих. Порівняння алгоритмів.

Тема 2.3. *Цифровий підпис.*

Алгоритми цифрового підпису. Порівняння алгоритмів.

Тема 2.4. *Нормативно-правове регулювання у галузі КЗІ*.

Державне регулювання господарських відносин у сфері криптографічного захисту інформації в Україні. Правове регулювання ЕЦП в Україні та світі. Державний контроль та право суспільства на криптографію. Міжнародні стандарти в сфері КЗІ. Стандартизація в сфері КЗІ в Україні

Тема 2.5. *Основні напрямки розвитку сучасної криптографії.*

Шифрування на еліптичних кривих. Методи диференціального криптоаналізу. Квантова криптографія.

2. Рекомендована література

Основна:

1. Венбо Мао. Современная криптография. Теория и практика. М: Вильямс, 2005. – 768 с.

2. Бернет С., Пэйн С., Криптография. Официальное руководство RSA Security. Изд. 2-е, стереотипное. – М.: ООО «Бином-Пресс», 2007. – 384 с.: ил.

3. Аграновский А.В., Хади Р.А. Практическая криптография: алгоритмы и их программирование. – М.: СОЛОН-Пресс, 2002. – 256 с.

4. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов. – М.: ДМК Пресс, 2012. – 256 с.

5. Бабаш А. В. Криптография. – М.: СОЛОН-Пресс, 2007. – 511 с.

6. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии: Учебное пособие. М.: Горячая Линия - Телеком, 2002. – 175 с.

7. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. М.: Издательство: АНО НПО "Профессионал", 2005. – 480 с.

8. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001. – 480 с.

Додаткова:

1. Маховенко Е. Б. Теоретико-числовые методы в криптографии. М.: Гелиос АРВ, 2006. – 320 с.

2. Мухачев В.А., Хорошко В.А. Методы практической криптографии. К.: ООО Полиграф-Консалдинг, 2005. – 209 с.

3. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М.: Горячая линия – Телеком, 2005. – 229 с.

4. Ростовцев А.Г. Алгебраические основы криптографии. М.: НПО «Мир и семья», ООО «Интерлайн», 2000. – 256 с.

5. Погорелова Б.А. Словарь криптографических терминов. М.: МЦНМО, 2006. – 94 с.

4. Форма підсумкового контролю успішності навчання

Денна форма навчання – підсумковий модульний контроль, залік в кінці 3 семестру.

5. Засоби діагностики успішності навчання

Оцінювання студентів проводяться згідно тематики вивчення дисципліни. Ці заходи мають на меті поглибити та закріпити знання, отримані студентами на лекціях, лабораторних роботах та в процесі самостійної роботи над навчальною та науковою літературою, рекомендованою викладачем, а також виробити у тих, хто навчається, уміння пошуку, узагальнення та викладання навчального матеріалу.

Підсумкові бали (оцінки) за кожне заняття вносяться викладачем до журналу занять навчальної групи. Одержані ними оцінки за окремі заняття враховуються при визначенні підсумкової оцінки (рейтингу) з даної навчальної дисципліни. Проводиться поточний контроль (усне та письмове опитування), виконання лабораторних завдань, підсумковий письмовий тест, залік в кінці 3-го семестру.