МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Інститут комп'ютерних інформаційних технологій
Кафедра безпеки інформаційних технологій

ЗАТВЕРДЖУЮ
Ректор університету
_____ М.Кулик
"_____"_____2014р.

Система менеджменту якості

НАВЧАЛЬНА ПРОГРАМА

навчальної дисципліни
«Новітні технології захисту інформації»

(за кредитно-модульною системою)

Напрям:	6.040301	«Прикладна математика»
Спеціальність :	7.04030101	«Прикладна математика»
	8.04030101	«Прикладна математика»

Курс – 5

Семестр – 9

Аудиторні заняття – 34
Самостійна робота – 72
Індивідуальні заняття – 2
Усього (годин/кредитів ECTS) – 108/3

Диференційований залік – 9 семестр

Індекс Н14 - 7.04030101 / 12-4.1.2
Н14 - 8.04030101 / 12-4.1.2

СМЯ НАУ НП 09.01.08-01-2014

Навчальна програма дисципліни «Новітні технології захисту інформації» розроблена на основі освітньо-професійної програми та навчальних планів № НС-14-7.04030101/12, № НМ-14-8.04030101/12 підготовки фахівців освітньо-кваліфікаційних рівнів «Спеціаліст», «Магістр» за напрямом 6.040301 «Прикладна математика» спеціальності 7/8.04030101 «Прикладна математика», «Тимчасового Положення про організацію навчального процесу за кредитно-модульною системою (в умовах педагогічного експерименту) » та «Тимчасового Положення про рейтингову систему оцінювання», затверджених наказом ректора від 15.06.2004 №122/од, та наказу ректора від 12.04.2005 №81/од.

Навчальну програму розробили:
доцент кафедри безпеки
інформаційних технологій _____ В. Ковтун
доцент кафедри безпеки
інформаційних технологій _____ В. Кінзерявий

Навчальна програма обговорена та схвалена на засіданні кафедри безпеки інформаційних технологій, протокол № ___ від _____ 2014 р.

Завідувач кафедри_____ О. Корченко

Навчальна програма обговорена та схвалена випусковою кафедрою напряму 6.040301 «Прикладна математика» (спеціальність 7/8.04030101 «Прикладна математика») – кафедри прикладної математики, протокол № ___ від «___» _____2014 р.

Завідувач кафедри_____ П. Приставка

Навчальна програма обговорена та схвалена на засіданні науково-методично-редакційної ради інституту комп'ютерних інформаційних технологій, протокол №_____ від "_____"_____ 2014 р.

Голова НМРР_____ Б. Масловський

УЗГОДЖЕНО
Директор ІКІТ

_____ О. Юдін

"_____"_____2014р.

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Контрольний примірник

ЗМІСТ

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

1.1. Місце навчальної дисципліни в системі професійної підготовки фахівця

Дисципліна «Новітні технології захисту інформації» є спеціальним курсом, що належить до циклу дисциплін вільного вибору студента.

Предметом вивчення дисципліни «Новітні технології захисту інформації» є методи, алгоритми та засоби криптографічного захисту інформації, методи, алгоритми та засоби криптоаналітичного відтворення захищеної інформації із застосуванням обчислювальної техніки.

Дисципліна «Новітні технології захисту інформації» повинна дати студентам знання і навички для вивчення і засвоєння подальших дисциплін, пов'язаних з захистом інформації та її обробкою, у значній мірі визначає рівень загальнонаукової підготовки спеціалістів і становить базову основу для вивчення принципів, методів, алгоритмів та обчислювальних технологій обробки інформації з обмеженим доступом із застосуванням електронно-обчислювальних машин (ЕОМ).

1.2. Мета виконання навчальної дисципліни

Основна мета дисципліни «Новітні технології захисту інформації» полягає в створенні як теоретичної, так і практичної бази для засвоєння та розвитку практичних навиків та умінь з захисту інформації, математичних методів та алгоритмів криптографічного перетворення даних із застосуванням ЕОМ у автоматизованих системах управління із заданим ступенем надійності та швидкодії.

1.3. Завдання вивчення навчальної дисципліни

Завдання вивчення дисципліни визначаються вимогами до підготовки спеціалістів та магістрів за спеціальністю 7/8.04030101 «Прикладна математика».

Головне завдання вивчення дисципліни полягає в висвітленні нових аспектів теорії інформації, теорії інформаційної безпеки та криптографічного перетворення даних, що виникають у зв'язку з можливостями застосування обчислювальної техніки, сучасних прикладних методів перетворення інформації із застосуванням комп'ютерних технологій, зокрема, криптографічні перетворення за допомогою ЕОМ із заданими властивостями, криптоаналітичної оцінки стійкості криптографічних перетворень, оцінка вразливості підсистем захисту інформації у автоматизованих систем до атак зловмисників, збір та первинна обробка інформації з виробленням оптимальних рішень та управляючих впливів.

Завдання вивчення навчальної дисципліни є:

- аналіз захищеності інформаційних ресурсів;
- створення криптографічних систем захисту інформації;
- реалізація захищеного електронного документообігу.

1.4. Інтегровані вимоги до знань та умінь з навчальної дисципліни

У результаті вивчення дисципліни студент повинен:

Знати:

- Основні теоретичні положення та визначення.
- Канали несанкціонованого отримання та руйнування інформації. Технічні канали витоку інформації. Класифікація, причини та джерела утворення. Методи та способи виявлення.
- Основи побудови криптосистем: безумовно стійкі, обчислювально-стійкі, доведено стійкі.
- Основні методи та алгоритми формування псевдовипадкових послідовностей та чисел із заданими характеристиками. Дослідження їх характеристик.
- Основи побудови симетричних криптосистем: блочні шифри, поточні шифри.

- Основи побудови криптосистем з відкритим ключем. Обчислення образу інформації (повідомлення) за допомогою геш-функції. Обмін ключами та вироблення спільного секрету. Формування та перевірка електронного цифрового підпису. Направлене блокове шифрування.
- Складно-обчислювальні задачі: Криптосистеми у полях та кільцях. Формування загальносистемних параметрів. Криптосистеми на еліптичних кривих. Формування загальносистемних параметрів. Криптосистеми на гіпереліптичних кривих. Формування загальносистемних параметрів.
- Методи криптоаналізу симетричних криптографічних алгоритмів (шифрів): блочних та поточних шифрів.
- Методи криптоаналізу геш-функцій.
- Методи криптоаналізу складно-обчислювальних задач, що покладені у основу криптографічних алгоритмів с відкритим ключем. Криптосистеми у полях та кільцях. Криптосистеми на еліптичних кривих. Криптосистеми на гіпереліптичних кривих.
- Сучасні криптографічні алгоритми. Блочні симетричні шифри: DES, ГОСТ 28147-89, AES. Поточні симетричні шифри: SNOW, у поточному режимі: DES, ГОСТ 28147-89, AES. Геш-функції: ГОСТ Р34.11-94, RIPEMD160, MD5. Електронний цифровий підпис: RSA, DSA, ECDSA, ДСТУ 4145-2002, ECGDSA, ECKDSA. Обмін ключами: ECKAS-DH1, ECKAS-DH2, ECKAS-MQV. Направленого шифрування: RSA, El-Gamal.
- Підходи до створення комплексної системи захисту інформації.

Вміти:

- Аналізувати характеристики та класифікувати джерела інформації.
- Досліджувати псевдовипадкові послідовності з використанням пакету NIST STS.
- Використовувати сучасні криптографічні бібліотеки, що інтегровані до операційних систем: Crypto Service Provider у операційних системах сімейства Windows для симетричного шифрування (DES, AES), з відкритими ключем (RSA шифрування та ЕЦА, ЕЦП за DSA та ECDSA.
- Використовувати сучасні криптографічні бібліотеки Intel Performance Primitives Crypto Package для реалізації: симетричного шифрування AES, GOST 28147-89. Асиметричного шифрування RSA, El-Gamal. Електронного цифрового підпису ECDSA та DSTU 4145-2002.
- Формулювати вимоги до підсистеми захисту інформації систем обробки інформації з обмеженим доступом.

1.5. Інтегровані вимоги до знань і умінь з навчальних модулів

Навчальний матеріал дисципліни структурований за модульним принципом і складається з одного навчального модуля.

1.5.1. У результаті засвоєння навчального матеріалу навчального модуля №1 «Основні поняття та симетричні криптосистеми. Асиметричні криптосистеми та особливості побудови криптографічних систем захисту інформації» студент повинен:

Знати:

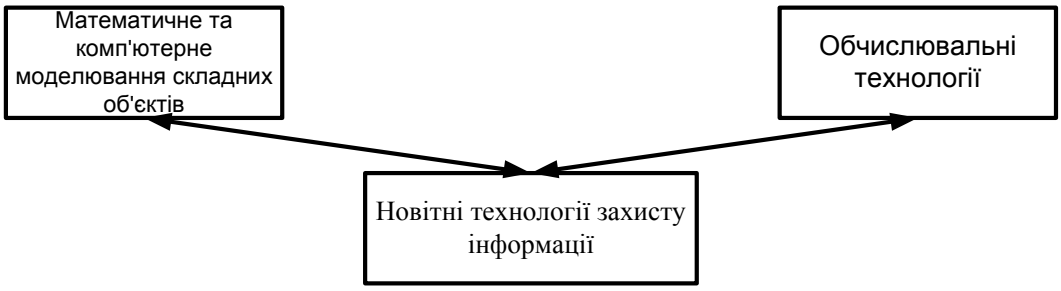
- Основні теоретичні положення та визначення.
- Канали несанкціонованого отримання та руйнування інформації. Технічні канали витоку інформації. Класифікація, причини та джерела утворення. Методи та способи виявлення.

- Основи побудови криптосистем: безумовно стійкі, обчислювально-стійкі, доведено стійкі.
- Основні методи та алгоритми формування псевдовипадкових послідовностей та чисел із заданими характеристиками. Дослідження їх характеристик.
- Основи побудови симетричних криптосистем: блочні шифри, поточні шифри. Сучасні криптографічні алгоритми. Блочні симетричні шифри: DES, ГОСТ 28147-89, AES. Поточні симетричні шифри: SNOW, у поточному режимі: DES, ГОСТ 28147-89, AES.
- Методи криптоаналізу симетричних криптографічних алгоритмів: блочних та поточних шифрів.
- Основи побудови асиметричних криптосистем (з відкритим ключем): геш-функції, ЕЦП, обмін ключами, направлене шифрування.
- Основні асиметричні криптографічні алгоритм (з відкритим ключем). Геш-функції: ГОСТ Р34.11-94, RIPEMD160, MD5. Електронний цифровий підпис: RSA, DSA, ECDSA, ДСТУ 4145-2002, ECGDSA, ECKDSA. Обмін ключами: ECKAS-DH1, ECKAS-DH2, ECKAS-MQV. Направленого шифрування: RSA, El-Gamal.
- Методи криптоаналізу геш-функцій.
- Методи криптоаналізу складно-обчислювальних задач, що покладені у основу криптографічних алгоритмів с відкритим ключем. Криптосистеми у полях та кільцях. Криптосистеми на еліптичних кривих. Криптосистеми на гіпереліптичних кривих.
- Підходи до створення комплексної системи захисту інформації.

Вміти:

- Аналізувати характеристики та класифікувати джерела інформації.
- Досліджувати псевдовипадкові послідовності з використанням пакету NIST STS.
- Використовувати сучасні криптографічні бібліотеки, що інтегровані до операційних систем: Crypto Service Provider у операційних системах сімейства Windows для симетричного шифрування (DES, AES).
- Використовувати сучасні криптографічні бібліотеки, що інтегровані до операційних систем: Crypto Service Provider у операційних системах сімейства Windows для симетричного шифрування (DES, AES), з відкритими ключем (RSA шифрування та ЕЦА, ЕЦП за DSA та ECDSA.
- Використовувати сучасні криптографічні бібліотеки Intel Performance Primitives Crypto Package для реалізації: симетричного шифрування AES, GOST 28147-89. Асиметричного шифрування RSA, El-Gamal. Електронного цифрового підпису ECDSA та DSTU 4145-2002.
- Формулювати вимоги до підсистеми захисту інформації систем обробки інформації з обмеженим доступом.

1.6. Міждисциплінарні зв'язки навчальної дисципліни



2. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1. Модуль №1 "Основні поняття та симетричні криптосистеми. Асиметричні криптосистеми та особливості побудови криптографічних систем захисту інформації".

Тема 2.1.1. Основні теоретичні положення та визначення. Канали несанкціонованого отримання та руйнування інформації.

Канали розповсюдження інформації. Канали несанкціонованого отримання інформації. Автоматизовані системи обробки інформації. Основні поняття та визначення захисту інформації. Симетричні криптосистеми. Асиметричні криптосистеми. Особливості побудови криптографічних систем захисту інформації.

Тема 2.1.2. Генератори випадкових та псевдовипадкових послідовностей. Статистичні тести. Криптографічно безпечні генератори псевдовипадкових послідовностей.

Випадкові числа. Генератори випадкових чисел. Генератори псевдовипадкових послідовностей. Використання стандартних функцій мов програмування високого рівня. Конгруентний генератор псевдовипадкових чисел. Лінійні регістри зі зворотним зв'язком (LFSR). Модифіковані LFSR.

Криптографічно стійкі датчики випадкових чисел. Системно-теоретичний підхід отримання випадкових чисел. Складно-теоретичний підхід отримання випадкових чисел. Інформаційно-теоретичний підхід отримання випадкових чисел. Рандомізований підхід отримання випадкових чисел. Генератори справжніх випадкових чисел. Відхилення та кореляції. Розподіл випадковості за допомогою односторонньої хеш-функції. Статистичні тести.

Тема 2.1.3. Симетричні криптосистеми. Блочний шифр: ГОСТ 28-147-89, AES. Поточний шифр: SNOW.

Симетричні криптосистеми. Симетрична криптосистема AES. Симетрична блокова криптосистема ГОСТ 28147-89. Потокові шифри.

Тема 2.1.4. Криптоаналіз симетричних криптосистем.

Універсальні методи криптоаналізу. Атака по ключам. Частотний аналіз. Методи криптоаналізу блочних шифрів. Методи криптоаналізу потокових шифрів. Криптоаналіз по побічним каналам. Стійкість сучасних стандартів симетричного шифрування. Використання нових технологій в криптоаналізі.

Тема 2.1.5. Асиметричні криптосистеми (з відкритим ключем). Геш-функції. ЕЦП. Направлене шифрування. Обмін ключами.

Застосування криптосистем з відкритим ключем. Умови застосування криптосистем з відкритим ключем. Криптосистема RSA. Криптосистема Ель-Гамаля. Односпрямовані геш-функції. Криптоперетворення в групах точок еліптичних кривих.

Тема 2.1.6. Криптоаналіз асиметричних криптосистем.

Криптоаналіз асиметричних криптосистем. Криптоаналіз геш-функцій. Рішення завдання факторизації. Рішення задачі дискретного логарифма. Квантові обчислення.

Тема 2.1.7. Підходи до створення комплексної системи захисту інформації.

Поняття захисту. Системність підходу. Труднощі реалізації систем захисту інформації. Основні правила захисту. Захищена інформаційна система та система захисту інформації. Вимоги до систем захисту інформації.

3. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

3.1. Основні рекомендовані джерела

3.1.1. В.А. Хорошко, А.А. Чекотков. Методы и средства защиты информации. –Юниор, 2003. 479 с.

3.1.2. Столингс В. Криптография и защита сетей: принципы и практика. 3-е издание. –М: Издательский дом «Вильямс», 2001. –672 с.

3.1.3. К. Шеннон. Теория связи в секретных системах // Работы по теории информации и кибернетике. М., ИЛ, 1963. -с. 333-369.

3.1.4. Intel Performance Primitives. User manual. URL: http://www.intel.com

3.1.5. В.В. Домарев. Безопасность информационных технологий. Методология создания систем защиты. — К.: ООО “ДС”, 2001. 688 с.

3.1.6. В.В. Домарев. Защита информации и безопасность компьютерных систем. К.: Издательство ДиаСофт, 1999. 480 с.

3.2. Додаткові рекомендовані джерела

3.2.1. H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren. Handbook of elliptic and hyperelliptic curve cryptography// Kenneth H. Rosen Ed. 2006. 843 p.

3.2.2. О.В. Казарин. Теория и практика защиты программ. М.: МГУЛ, 2003. 450 с.

3.2.3. Microsoft Software Development Network. URL: http://www.msdn.com

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ пор.	Прізвище ім'я по-батькові	Підпис ознайомленої особи	Дата ознайом-лення	Примітки

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	Зміненого	Заміненого	Нового	Анульо-ваного			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				