Національний університет «Чернігівська політехніка»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра *інформаційних технологій та програмної інженерії*

“**ЗАТВЕРДЖУЮ**”
Завідувач кафедри

Білоус Ірина Володимирівна

“_____”_____20__ р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КОДУВАННЯ ТА ЗАХИСТ ІНФОРМАЦІЇ (ВБ8.2)

Освітня програма «*Інженерія програмного забезпечення*»

Рівень вищої освіти – *перший (бакалаврський)*

Спеціальність *121 – Інженерія програмного забезпечення*

Мова навчання: *українська*

Статус дисципліни: *вибіркова*

Форма навчан.	Рік навч.	Сем	Розподіл годин				Разом	За тиждень		ІНДЗ	Контр.
			Всього ауд.	Лек	Лаб.	СРС		Ауд.	СРС		
Денна	3	6	30	16	14	90	120	1,85	5,6	РГР	І

Чернігів – 2020 рік

Робоча програма ___*Кодування та захист інформації*_____
(назва навчальної дисципліни)
для студентів галузі знань 12 – «Інформаційні технології»
спеціальності 121 – «Інженерія програмного забезпечення»

Розробник робочої навчальної програми:
старший викладач кафедри інформаційних технологій та програмної інженерії

_____ (*В.В. Нехай)*
(підпис) (прізвище та ініціали)

Робоча програма схвалено на засіданні кафедри *інформаційних технологій та програмної інженерії*

Протокол від "__" _____ *20*__ року № __

Завідувач кафедри *інформаційних технологій та програмної інженерії*

_____ (__*І.В.Білоус*__)
(підпис) (прізвище та ініціали)

Abstract

ESIEIT/PI ВБ8.2 Encryption and protection of information
2020/2021 Sem. 6 2020/2021 Sem. 6
Course Description

The date successful work of enterprises and organizations depends all in a greater measure from informative resources. The value of informative is determined by her authenticity, actualsty and confidentiality. The wideuse of computer facilities in human activity resulted in the origin of important task of providing of effective exploitation of the systems of storage and treatment of information. On the first plan the question of defence of information goes out from unauthorized influences.

Contents: A course “Encryption and protection of information” puts the aim receipt by the students of theoretical knowledge, practical skills in area of decision of task of defence of information in composition the computer informative systems. The students it is offered to study both classic and modern methods and facilities, applied for defenct of information.

Application of the computer system of study of methods and facilities of hardwarily-programmatic defence of information, futher computer system, allows to promote efficiency of educating for an account.

1 Опис навчальної дисципліни

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th></tr>
<tr><td>Кількість кредитів – 4</td><td>Галузь знань
12 Інформаційні технології</td><td>Обов’язкова</td></tr>
<tr><td>Модулів – 1</td><td rowspan="4">Спеціальність:
121 – Інженерія програмного забезпечення
Освітньо-професійна програма:
Інженерія програмного забезпечення</td><td>Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 3</td><td>3-й</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 120</td><td>Семестр</td></tr>
<tr><td>6-й</td></tr>
<tr><td rowspan="8">Тижневих годин:
аудиторних – 1,8;
самостійної роботи і індивідуальної студента – 5,6;</td><td rowspan="8">Освітньо-кваліфікаційний рівень:
бакалавр</td><td>Лекції</td></tr>
<tr><td>16</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>14</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>90</td></tr>
<tr><td>Вид контролю:</td></tr>
<tr><td>Іспит</td></tr>
</table>

Примітка.

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить:
у 6-му семестрі – 1,875: 5,625=1:3.

Навички, що необхідні для виконання лабораторних та домашніх завдань в межах дисципліни, студенти отримують з дисциплін «Комп’ютерна дискретна математика», що викладалися раніше.

2 Мета та завдання навчальної дисципліни

Метою викладання дисципліни «Кодування та захист інформації» є отримання теоретичної бази, яка необхідна при засвоєнні прикладних питань одержання знань з типових методів, алгоритмів та технологій захисту інформації.

Особливості систем, що проектуються, обумовлюють різноманітність підходів до розробки різних способів захисту систем. Тому основний наголос у курсі зроблено на вивченні алгоритмів традиційних криптосистем, що відповідає вимогам кваліфікаційної характеристики фахівця.

Під час вивчення дисципліни здобувач вищої освіти (ЗВО) має набути або розширити наступні загальні (ЗКх) та фахові (ФКх) компетентності, передбачені освітньою програмою:

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК31. Здатність працювати в міжнародному контексті.

ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ФК19. Здатність дотримуватися специфікацій, стандартів, правил і рекомендацій в професійній галузі при реалізації процесів життєвого циклу.

ФК20. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

ФК28. Здатність до алгоритмічного та логічного мислення.

3 Очікувані результати навчання з дисципліни

Навчальна дисципліна “Кодування та захист інформації” має допомогти сформувати наступні програмні результати навчання.

– ПР01. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.

– ПР07. Знати і застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування мовних, інструментальних і обчислювальних засобів інженерії програмного забезпечення.

– ПР12. Застосовувати на практиці ефективні підходи щодо проектування програмного забезпечення.

– ПР13. Знати і застосовувати методи розробки алгоритмів, конструювання програмного забезпечення та структур даних і знань.

– ПР15. Мотивовано обирати мови програмування та технології розробки для розв'язання завдань створення і супроводження програмного забезпечення.

– ПР18. Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних.

– ПР21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

Після вивчення дисципліни студенти **повинні знати*:***

– основні положення законодавства в галузі захисту інформації, основні міжнародні та національні стандарти з безпеки інформаційних систем (ІС) та технологій (Т);

– основні терміни та визначення політики безпеки, принципи побудови профілю захисту інформації для забезпечення послуг безпеки;

– принципи роботи сучасних криптосистем, основні тенденції розвитку сучасних криптосистем;

– механізми та протоколи забезпечення конфіденціальності ІС та Т;

– механізми та протоколи забезпечення автентичності ІС та Т; механізми та протоколи забезпечення цілісності даних ІС та Т; модель порушника, основні види атак, принципи крипто аналізу; механізми та протоколи керування ключами в ІВК інформаційної системи; методи та процедури цифрової стеганографії.

У результаті опанування навчальною дисципліною студенти **повинні вміти** :

– аналізувати вимоги безпеки в комп’ютерних мережах;

– застосовувати на практиці різні типи традиційних симетричних криптосистем;

– розробляти та втілювати в програмах алгоритми рішення задач захисту інформації у комп’ютерних мережах.

4 Критерії оцінювання результатів навчання

До іспиту допускаються здобувачі вищої освіти, що виконали усі заплановані на семестр завдання з підсумковою оцінкою не менше 20 балів.

З тими здобувачами вищої освіти, які до проведення підсумкового семестрового контролю не встигли виконати всі обов’язкові види робіт та мають підсумкову оцінку менше 20 балів (за шкалою оцінювання), проводяться додаткові індивідуальні заняття, за результатами яких визначається, наскільки глибоко засвоєний матеріал, та чи необхідне повторне вивчення дисципліни.

Дисципліну можна вважати такою, що засвоєна, якщо студент:

1) знає:

– класифікацію та основні параметри традиційних симетричних криптосистем;

– основні алгоритми сучасних симетричних криптосистем;

– основи побудови сучасних асиметричних криптосистем;

– сучасні протоколи ідентифікації;

– алгоритми безпечного хешування;

– алгоритми електронного цифрового підпису.

2) вміє:

– розшифровувати повідомлення, яке зашифроване симетричним шифром;
– розшифровувати повідомлення, яке зашифроване асиметричним шифром;
– перевіряти цифровий підпис під отриманим документом.

5 Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з дисципліни є:

– екзамен;
– розрахунково-графічна робота;
– презентації результатів виконаних завдань;
– завдання, які виконуються в навчальній лабораторії.

6 Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1 – Симетричні криптосистеми

Вступ

Предмет та завдання курсу «Захист інформації у комп’ютерних системах».

Класифікація складових частин та їхні особливості. Основні етапи вивчення дисципліни.

Інформаційна безпека комп’ютерних систем

Основні поняття та визначення. Основні загрози безпеки. Забезпечення безпеки. Принципи криптографічного захисту інформації.

Традиційні симетричні криптосистеми

Основні поняття та визначення. Шифри перестановки: "скітала", шифруючи таблиці, магічні квадрати. Шифри простої заміни: полібіанський квадрат, системи Цезаря, таблиці Трисемуса, біграмний шифр Плейфера, система омофонів.

Шифри складної заміни: шифр Гронсфельда, система Віжінера, "подвійний квадрат" Уітстона, одноразова система шифрування, роторні машини.

Шифрування методом гамування.

Сучасні симетричні криптосистеми

Стандарт шифрування данних DES. Основні режими роботи алгоритму: електронна кодова книга, зчеплення блоків шифру, зворотній зв'язок по шифру, зворотній зв'язок по виходу.

Комбінування блочних алгоритмів.

Міжнародний алгоритм шифрування даних IDEA.

Російський стандарт шифрування даних ГОСТ 28147-89. Режим простої заміни: шифрування і розшифрування даних. Режими гамування та гамування зі зворотнім зв’язком. Режим виробітки імітовставки.

Блочні та поточні шифри.

Змістовий модуль 2 – Асиметричні криптосистеми

Сучасні криптосистеми з відкритим ключем

Концепція криптосистеми з відкритим ключем. Односпрямовані функції. Вступ в теорію чисел.

Криптосистема шифрування даних RSA. Процедури шифрування і розшифрування. Безпека та швидкодія RSA.

Схеми шифрування Поліга-Хеллмана та Ель-Гамаля.

Комбінований метод шифрування.

Ідентифікація та перевірка автентичності

Основні поняття та концепції. Ідентифікація і механізми підтвердження автентичності користувача. Взаємна перевірка автентичності користувачів.

Протоколи ідентифікації з нульовим переданням знань: спрощена та паралельна схема, схема Гіллоу-Куікскуотера.

Алгоритми хешування

Односпрямовані хеш-функції на основі симетричних блочних алгоритмів.

Алгоритм MD5 числення профілю повідомлення. Логіка. Функція стискування. Стійкість.

Захищений алгоритм хешування SHA-1. Логіка. Функція стискування.

Порівняльний аналіз SHA та MD5.

Російський стандарт хеш-функції ГОСТ Р 34.11-94.

Алгоритм електронного цифрового підпису

Алгоритм цифрового підпису RSA. Алгоритм цифрового підпису EGSA (Ель-Гамаля). Алгоритм цифрового підпису DSA.

Російський стандарт цифрового підпису ГОСТ Р 34.10-94.

Змістовий модуль 3 – Захист від мережевих атак

Управління криптографічними ключами

Генерація ключів. Зберігання ключів. Розподілення ключів: з участю центра розподілення ключів, прямий обмін ключами між користувачами.

Методи та засоби захисту від віддалених атак через мережу Internet

Особливості функціювання міжмережних екранів. Основні компоненти міжмережних екранів: фільтруючі маршрутизатори, шлюзи мережевого рівня, шлюзи прикладного рівня, посилена автентифікація.

Основні схеми мереженого захисту на базі міжмережних екранів: міжмережний екран – фільтруючий маршрутизатор, міжмережний екран на основі двупортового шлюзу, міжмережний екран на основі екранованого шлюзу, міжмережний екран – екранована підмережа. Застосування міжмережних екранів для організації віртуальних корпоративних мереж.

Програмні методи захисту

7 Структура навчальної дисципліни

Назви змістових модулів і тем		Кількість годин для денної форми навчання				
		Всього	У тому числі			
			Лек.	Пр.	Лаб.	С.р.
1	**2**	**3**	**4**	**5**	**6**	**7**
Модуль 1						
Змістовий модуль 1 Симетричні криптосистеми						
1	Вступ	3	1			2
2	Інформаційна безпека комп'ютерних систем	7	1			6
3	Традиційні симетричні криптосистеми	10	2		2	6
4	Сучасні симетричні криптосистеми	8	2			6
Разом за змістовим модулем 1		**28**	**6**		**2**	**20**
Змістовий модуль 2 Асиметричні криптосистеми						
5	Сучасні криптосистеми з відкритим ключем	11	1		2	8
6	Ідентифікація та перевірка автентичності	11	1		2	8
7	Алгоритми хешування	12	2		2	8
8	Алгоритм електронного цифрового підпису	12	2		2	8
Разом за змістовим модулем 2		**42**	**6**		**8**	**28**
Змістовий модуль 3. Захист від мережевих атак						
9	Поняття ресурсу. Дисципліни розподілення ресурсів	10	2		2	6
10	Управління оперативною пам'яттю	10	2		2	6
11	РГР	30	-		-	30
Разом за змістовим модулем 3		**50**	**4**		**4**	**42**
Усього годин за дисципліну		**120**	**16**		**14**	**90**

8 Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
Модуль 1		
1	Вступне заняття. Вступний інструктаж з техніки безпеки.	1
2	Дослідження шифрів перестановки та простої заміни.	2
3	Аналіз вимог безпеки.	2
4	Сучасні алгоритми симетричного шифрування.	2
5	Алгоритми шифрування з відкритим ключем.	2
6	Средства ідентифікації та автентичності, електронний цифровий підпис.	2
7	Формальні політики безпеки.	2
8	Заключне заняття. Здача звіту лабораторних робіт за семестр.	1
Разом		**14**

9 Самостійна робота

№ з/п	Назва теми	Кількість Годин
1	Інформаційна безпека комп’ютерних систем	4
2	Традиційні симетричні криптосистеми	6
3	Сучасні симетричні криптосистеми	6
4	Сучасні криптосистеми з відкритим ключем	8
5	Ідентифікація та перевірка автентичності	8
6	Алгоритми хешування	8
7	Алгоритм електронного цифрового підпису	8
8	Управління криптографічними ключами	6
9	Методи та засоби захисту від віддалених атак через мережу Internet	6
10	РГР	30
	Разом	**90**

10 Індивідуальні завдання

Метою розрахунково-графічних робіт є перевірка засвоєння студентами отриманого на лекціях та лабораторних роботах матеріалу та вміння самостійно вирішувати типові задачі за прослуханими темами. Варіанти завдань до даних робіт містяться в відповідних методичних вказівках.

Форми контролю виконання РГР

Вид роботи	Форма контролю	Кількість балів
Структура системи, схема та текст програми	1. Відповідність умовам завдання 2. Відповідність вимогам стандартів	0… 4 0… 2
Пояснювальна записка	1. Обґрунтованість програмних рішень 2. Посилання на першоджерела 3. Відповідність оформлення вимогам 4. Своєчасність здачі	0… 4 0… 1 0… 2 0… 2
Захист РГР	Самостійність виконання (відповіді на запитання або презентація)	0… 5
Разом		**0… 20**

11 Методи контролю

Оцінювання знань студентів здійснюється відповідно до «Положення про поточне та підсумкове оцінювання знань студентів Чернігівського національного технологічного університету», погодженого вченою радою ЧНТУ (протокол № 9 від 26.10.2015 р.) та затвердженого наказом ректора ЧНТУ від 29.10.2015 р. №181.

Лекційний матеріал подається у вигляді презентацій за допомогою медіа-проектора. Під час лекцій аналізуються проблемні ситуації, організується зворотний зв'язок з аудиторією шляхом формулювання запитань у режимі діалогу.

Під час лабораторних занять коротко розглядаються теоретичні положення відповідно до тематичного плану занять, докладно розбираються приклади, а надалі студентами самостійно вирішуються практичні задачі. Особливістю виконання лабораторних робіт є застосування спеціального обладнання та системного програмного забезпечення навчальних лабораторій.

Переліки екзаменаційних питань знаходяться в пакеті документів на дисципліну. У випадку, якщо студент протягом семестру не виконав в повному обсязі передбачених робочою програмою всіх видів навчальної роботи, має невідпрацьовані лабораторні роботи або не набрав мінімально необхідну кількість балів (20), він не допускається до складання екзамену під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань студентів ЧНТУ».

Повторне складання екзамену з метою підвищення позитивної оцінки не дозволяється.

12 Розподіл балів, які отримують студенти

Поточний контроль за модулями

	Змістовний модуль 1	**М1=0…100**
1	Робота на лекціях з вивчення лекційного матеріалу	0…10
2	Виконання та захист лабораторних робіт	0…40
3	Тестування з вивчення теоретичного матеріалу	0…50
	Змістовний модуль 2	**М2=0…100**
1	Робота на лекціях з вивчення лекційного матеріалу	0…10
2	Виконання та захист лабораторних робіт	0…40
3	Тестування з вивчення теоретичного матеріалу	0…50
	Змістовний модуль 3	**М3=0…100**
1	Робота на лекціях з вивчення лекційного матеріалу	0…10
2	Виконання та захист лабораторних робіт	0…40
3	Тестування з вивчення теоретичного матеріалу	0…50
	РГР	**М4=0…100**

Ітогова оцінка Оцінка1 поточного контролю обчислюється як Оцінка1 = 60%*(М1+М2+М3+М4)/4.

Для *захисту лабораторної роботи* здобувач вищої освіти повинен відповісти на всі контрольні запитання з методичних вказівок та на два запитання за вибором викладача з лекційного курсу за темою лабораторної роботи. Для *денної форми навчання* за кожну лабораторну роботу студент отримує певну кількість балів з урахуванням максимальної кількості балів згідно наведеної вище таблиці. При цьому враховується якість оформлення звіту та повнота відповідей на запитання при захисті лабораторної роботи.

Для *захисту розрахунково-графічної роботи* здобувач вищої освіти повинен відповісти на всі контрольні запитання з методичних вказівок та на чотири за вибором викладача які стосуються безпосередньо варіанту завдання РГР.

Шкала оцінювання: національна та ECTS

<table>
<tr><th rowspan="2">Сума балів за всі види навчальної діяльності</th><th rowspan="2">Оцінка ECTS</th><th colspan="2">Оцінка за національною шкалою</th></tr>
<tr><th>для екзамену, курсового проекту</th><th>для заліку</th></tr>
<tr><td>90 – 100</td><td>A</td><td>відмінно</td><td rowspan="5">Зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>незадовільно з можливістю повторного складання</td><td>не зараховано з можливістю повторного</td></tr>
</table>

			складання
0-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

13 Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

Лекційний матеріал подається у вигляді презентацій за допомогою медіа-проектора. Під час лекцій аналізуються проблемні ситуації, організується зворотний зв'язок з аудиторією шляхом формулювання запитань і стислих відповідей з обох сторін.

Лабораторне заняття включає проведення поточного контролю підготовленості студентів до виконання конкретної лабораторної роботи, виконання завдань теми заняття, оформлення індивідуального звіту з виконаної роботи та його захисту перед викладачем.

Рекомендовані технології для реалізації лабораторних робіт– вільне модульне інтегроване середовище розробки програмного забезпечення Eclipse.

14 Методичне забезпечення

1. Використання алгоритмів криптосистем з відкритим ключем. Методичні вказівки до розрахунково-графічної роботи з дисципліни «Захист інформації в комп'ютерних системах та мережах» для студентів напрямку «Комп'ютерна інженерія». / Укл. Соломаха В. В., Павловський В.І., Верьовко О.В. – Чернігів: ЧДТУ, 2010. - 41 с.
2. Методичні вказівки до лабораторних робіт з дисципліни "Кодування та захист інформації " для студентів спеціальності 121 - "інженерія програмного забезпечення".

15 Рекомендована література

Базова

1. Подлевський Б. М. Теорія інформації в задачах: підручник / Б. М. Подлевський, Р. Є. Рикалюк. – Київ: «Центр учбової літератури», 2017. – 271 с.
2.Подлевський Б. М. Теорія інформації : підручник / Б. М. Подлевський, Р. Є. Рикалюк. – Львів: Видавничий центр ЛНУ ім. І. Франка, 2016. – 342 с.

Допоміжна

1. Основи теорії інформації та кодування. Конспект лекцій: [Електронний ресурс]: навч. посіб. для студ. спеціальності 171 «Електроніка», спеціалізації «Електронні та інформаційні системи і технології телебачення, кінематографії та звукотехніки»/ М.І. Романюк; Ю. Г. Савченко; КПІ ім. Ігоря Сікорського. – Електронні текстові данні (1 файл: 1,86 Мбайт). – Київ: КПІ ім. Ігоря Сікорсь-

кого, 2019. –70 с.
2. Теорія інформації та кодування [Текст]: навч. посібник / В.Л. Кожевников, А.В. Кожевников. – Д.: Національний гірничий університет, 2011. – 108 с

16 Інформаційні ресурси

1. Unit: Information theory [Електронний ресурс]. – Режим доступу: https://www.khanacademy.org/computing/computer-science/informationtheory