

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ М.П. ДРАГОМАНОВА**

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ОСВІТНІХ ВИМІРЮВАНЬ

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ

ПРОГРАМА

навчальної дисципліни

підготовки магістра

галузь знань **01 Освіта/Педагогіка, 12 Інформаційні технології**

спеціальність **122 Комп'ютерні науки,**

**011 Освітні, педагогічні науки
(Освітні вимірювання)**

КИЇВ – 2019

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ М.П. ДРАГОМАНОВА**

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ОСВІТНІХ ВИМІРЮВАНЬ

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ

ПРОГРАМА

навчальної дисципліни

підготовки магістра

галузь знань **01 Освіта/Педагогіка, 12 Інформаційні технології**

спеціальність **122 Комп'ютерні науки,**

**011 Освітні, педагогічні науки
(Освітні вимірювання)**

КИЇВ – 2019

УДК 004.775-049.65(073)
3-38

*Рекомендовано до друку Вченою радою Факультету інформатики
Національного педагогічного університету імені М.П. Драгоманова
(протокол № 3 від 19 грудня 2018 р.).*

Рецензенти:

- Ю.В. Горошко доктор педагогічних наук, професор, завідувач кафедри інформатики і обчислювальної техніки Національний університет "Чернігівський колегіум" імені Т.Г. Шевченка.
- Л.О. Кухар кандидат педагогічних наук, доцент кафедри комп'ютерної інженерії та освітніх вимірювань, факультету інформатики НПУ імені М.П. Драгоманова.

3-38 Захист інформаційних ресурсів: програма навчальної дисципліни для підготовки студентів за спеціальністю «122 Комп'ютерні науки», «011 Освітні, педагогічні науки (Освітні вимірювання)» Факультету інформатики НПУ імені М.П. Драгоманова / укл. В.М. Франчук (в авторській редакції). - Київ: Вид-во НПУ імені М.П. Драгоманова, 2019 р. – 25 с.

В програмі наведено зміст навчальної дисципліни «Захист інформаційних ресурсів» для підготовки студентів за спеціальністю «122 Комп'ютерні науки», «011 Освітні, педагогічні науки (Освітні вимірювання)» Факультету інформатики НПУ імені М.П. Драгоманова. Програма складена за модульною схемою, наведено завдання вивчення навчальної дисципліни, вимоги до знань, навичок та умінь студентів, інформаційне наповнення, тематика лабораторних занять, зразки підсумкового контролю навчальних досягнень студентів, список рекомендованої літератури. Може бути використана для підготовки студентів фізико-математичних та інформатичних спеціальностей педагогічних закладів вищої освіти.

УДК 004.775-049.65(073)
© В.М. Франчук, 2019
© НПУ імені М.П. Драгоманова, 2019

ЗМІСТ

ВСТУП.....	4
1. Мета та завдання навчальної дисципліни.....	5
2. Інформаційний обсяг навчальної дисципліни	10
2.1. <i>Структура навчальної дисципліни</i>	10
2.2. <i>Теми лабораторних занять</i>	12
2.3. <i>Самостійна (індивідуальна) робота</i>	13
2.4. <i>Методичне забезпечення</i>	16
3. Рекомендована література.....	19
4. Форма підсумкового контролю успішності навчання.....	21
5. Засоби діагностики успішності навчання	23
ДЛЯ ЗАМІТОК	25

ВСТУП

Програма навчання нормативної дисципліни «*Захист інформаційних ресурсів*» складена відповідно до освітньо-професійної програми підготовки магістра з галузі знань «01 Освіта/Педагогіка» спеціальності 011 Освітні, педагогічні науки (Освітні вимірювання) та галузі знань «12 Інформаційні технології» спеціальностей «122 Комп'ютерні науки» і є основним документом, в якому визначається обсяг і орієнтовний порядок вивчення змістових модулів навчальної дисципліни відповідно до галузевого стандарту вищої освіти.

Навчання дисципліни «*Захист інформаційних ресурсів*» дає студентам необхідні теоретичні знання про основні принципи апаратно-програмних засобів захисту даних в комп'ютерних системах, криптографічних та стеганографічних методів захисту даних, що сприяє формуванню інформатичних компетентностей майбутніх фахівців.

Предметом навчання дисципліни є процес формування у майбутніх фахівців з розробки та тестування програмного забезпечення знань, умінь та навичок захисту програм та даних.

Міждисциплінарні зв'язки. Одним із важливих компонентів програми є міжпредметне узгодження. Курс «*Захист інформаційних ресурсів*» розрахований для студентів, що засвоїли базові математичні курси та вивчили дисципліни «Конструювання програмного забезпечення», «Архітектура комп'ютера», «Операційні системи», «Організація комп'ютерних мереж» і мають базові знання про склад і призначення основних компонентів обчислювальної техніки. Вивчення даного курсу забезпечує необхідний рівень знань для опанування дисциплінами «Якість програмного забезпечення та тестування», «Архітектура та проектування програмного забезпечення», «Програмування Інтернет».

Програма навчальної дисципліни «*Захист інформаційних ресурсів*» складається з таких змістових модулів:

- I. Апаратно-програмні засоби захисту даних в комп'ютерних системах.
- II. Криптографічні та стеганографічні методи захисту даних.

1. Мета та завдання навчальної дисципліни

Метою навчання дисципліни «Захист інформаційних ресурсів» є формування у студентів за напрямом підготовки бакалавра з галузі знань «01 Освіта/Педагогіка» спеціальності 011 Освітні, педагогічні науки (Освітні вимірювання) та галузі знань «12 Інформаційні технології» спеціальностей «122 Комп'ютерні науки» системи фундаментальних знань щодо свідомого, активного та вмілого використання нових інформаційних технологій захисту даних у процесі розробки та тестування програмного забезпечення..

Основними завданнями навчання дисципліни «Захист інформаційних ресурсів» є:

- розкрити місце і значення дисципліни в загальній і професійній діяльності;
- з'ясувати психолого-педагогічні аспекти засвоєння предмету, взаємозв'язки курсу з іншими навчальними дисциплінами, зокрема з інформатичними дисциплінами;
- навчити студентів ефективно захищати дані під час розробки та тестування програмного забезпечення;
- навчити майбутніх фахівців орієнтуватися у засобах захисту комп'ютерних систем, свідомо обирати тип, склад та конфігурацію обчислювальної техніки у відповідності до конкретних вимог використання цих систем;
- продемонструвати ефективність використання методів захисту програм та даних.
- розглянути криптографічні та стеганографічні методи захисту програм та даних.

Основні результати навчання і компетентності згідно з вимогами освітньо-професійної програми. Дисципліна є методичною і практичною основою сукупності знань та вмінь, необхідних майбутньому фахівцеві для виконання професійних завдань, пов'язаних з використанням апаратно-програмних засобів захисту даних в комп'ютерних системах у своїй професійній діяльності.

№ з/п	Результати навчання	Компетентності
1	Знати: – актуальні проблеми комп'ютерної	Соціально-особистісні: – здатність учитися;

<p>безпеки, цілісність даних, конфіденційність даних, доступність даних, розголошення даних, витік даних, захист даних, порушенням режиму доступу, несанкціонований доступ, об'єкт злочину, блокування даних, модифікація даних, одержання захищуваних даних, фільтрація даних, канал витоку даних, помилка, прорахунок, вразливість інформаційної системи, види загроз, джерела загроз, контроль безпеки, види атак, вторгнення, політика безпеки, класифікація навмисних загроз безпеки комп'ютерних систем;</p> <p>– стискування, архівація даних, архіватор, ступінь стискування, коефіцієнт стискування, методи стискування файлів, резервне копіювання, технології резервного копіювання;</p> <p>– перспективні розробки у сфері зберігання вмісту запам'ятовуючих пристроїв, технології захисту оптичних дисків від несанкціонованого копіювання, діагностика та профілактика жорстких магнітних дисків, технології захисту флеш-накопичувачів, засоби відновлення пошкодженого і втраченого вмісту запам'ятовуючих пристроїв, гарантоване вилучення вмісту запам'ятовуючих пристроїв;</p> <p>– вразливості програмного забезпечення та засоби боротьби з ними, дослідження вихідних текстів</p>	<p>– турбота про якість виконуваної роботи.</p> <p>Загальнонаукові:</p> <p>– базові знання в галузі захисту інформаційних ресурсів;</p> <p>– навички використання програмних засобів і навички роботи в комп'ютерних системах, уміння використовувати засоби захисту даних.</p> <p>Інструментальні:</p> <p>– навички роботи захисту даних під час роботи за комп'ютером;</p> <p>– навички роботи захисту даних під час роботи з інформаційними ресурсами;</p> <p>– дослідницькі навички у галузі захисту даних.</p> <p>Професійні:</p> <p>– розуміння тенденцій розвитку захисту інформаційних ресурсів;</p> <p>– вміння застосовувати захист інформаційних ресурсів в наукових дослідженнях та в професійній діяльності;</p> <p>– здатність до ділових</p>
---	--

<p>програмного забезпечення, захист програм встановлених на жорсткому диску, захист програм від вивчення;</p> <ul style="list-style-type: none"> – комп'ютерні віруси і засоби боротьби з ними, історія комп'ютерних вірусів, класифікація комп'ютерних вірусів, антивірусні програми, типи антивірусних програм, методи розпізнавання шкідливих об'єктів, захист комп'ютера від шпигунських програм; – мережеві атаки, види мережевих атак, сегментація мереж, міжмережеві екрани, списки управління доступом (ACL), загрози використання глобальної мережі Інтернет, методи захисту; – актуальні проблеми використання безпроводних мереж, типи загроз безпеці в безпроводних мережах, способи захисту даних в безпроводних мережах. <p>Вміти:</p> <ul style="list-style-type: none"> – використовувати засоби парольної ідентифікації в операційних системах, в програмних додатках, в мережевих сервісах, способи захисту від перебирання паролів, варіанти заміни традиційних паролів, способи створення складних паролів; – застосовувати засоби захисту і спеціалізовані програмні продукти для розв'язування типових проблем в галузі захисту інформаційних ресурсів; – кваліфіковано оцінювати 	<p>комунікацій у професійній сфері, знання основ ділового спілкування, здатність до роботи в команді для захисту інформаційних ресурсів.</p>
--	--

	<p>можливості застосування конкретних механізмів захисту;</p> <ul style="list-style-type: none"> – компетентно використовувати апаратні та програмні засоби захисту при розв'язуванні практичних задач. 	
2	<p>Знати</p> <ul style="list-style-type: none"> – поняття криптології, криптографії. Ключ, шифрування, зашифровування, розшифровування, криптостійкість, криптоаналіз, методи криптоаналізу, криптографічні методи захисту даних; – алгоритми шифрування, симетричні криптографічні алгоритми, асиметричні криптографічні алгоритми; – криптосистеми з відкритим ключем, електронний (цифровий) підпис, технології застосування систем електронного цифрового підпису, генерація ключів; – реалізації криптозахисту на апаратному рівні. Архітектура апаратних засобів криптозахисту. Організація інтерфейсу для роботи з прикладними програмами; – поняття стеганографії, історія стеганографії, стеганографічні методи і системи; – проблеми шифрування великих повідомлень, сучасні способи вирішення проблеми розподілу ключів, системи біометричної аутентифікації, перспективи використання криптографічних засобів захисту даних. <p>Вміти</p> <ul style="list-style-type: none"> – застосовувати симетричні 	<p>Соціально-особистісні:</p> <ul style="list-style-type: none"> – здатність учитися; – турбота про якість виконуваної роботи. <p>Загальнонаукові:</p> <ul style="list-style-type: none"> – базові знання в галузі захисту інформаційних ресурсів; – навички використання програмних засобів і навички роботи в комп'ютерних системах, уміння використовувати засоби захисту даних. <p>Інструментальні:</p> <ul style="list-style-type: none"> – навички роботи захисту даних під час роботи за комп'ютером; – навички роботи захисту даних під час роботи з інформаційними ресурсами; – дослідницькі навички у галузі захисту даних. <p>Професійні:</p> <ul style="list-style-type: none"> – розуміння тенденцій розвитку захисту інформаційних

Захист інформаційних ресурсів

	криптографічні алгоритми, асиметричні криптографічні алгоритми; – користуватися криптосистеми з відкритим ключем, електронний (цифровий) підпис, технології застосування систем електронного цифрового підпису, генерація ключів; – використовувати стеганографічні методи і системи.	ресурсів; – вміння застосовувати захист інформаційних ресурсів в наукових дослідженнях та в професійній діяльності; – здатність до ділових комунікацій у професійній сфері, знання основ ділового спілкування, здатність до роботи в команді для захисту інформаційних ресурсів.
--	---	--

Дисципліна «Захист інформаційних ресурсів» за навчальним планом підготовки бакалавра належить до нормативної складової циклу професійної та практичної підготовки. На вивчення курсу «Захист інформаційних ресурсів», який вивчається на 2 курсі (3 семестр), відводиться 3 кредити або 90 навчальні години, з яких 66 годин відведено на самостійну навчально-пізнавальну роботу студентів, а 24 години – на аудиторні заняття, які проводяться у формі лекційних занять (10 год.) та лабораторних робіт (14 год.). Самостійна робота полягає у підготовці до аудиторних занять, виконанні завдань, що пропонуються на лекційних та лабораторних заняттях, підготовці до модульного контролю тощо.

Назва дисципліни	Вид контролю	ECTS	Всього	Самостійна робота	Аудиторні	Лекції	Лабораторні	Індивідуальні
Захист інформаційних ресурсів	Залік	3	90	66	24	10	14	0

На лекційних заняттях розглядаються фундаментальні теоретичні питання з безпеки програм та даних; систематизуються, та

узагальнюються знання, навички та уміння набуті при вивченні суміжних дисциплін.

На лабораторних заняттях студенти знайомляться із сучасними програмними і апаратними засобами захисту даних, набувають уміння і навички роботи із ними. Одним із основних завдань при проведенні лабораторного практикуму є набуття умінь та навичок аналізу роботи програмного засобу та апаратного забезпечення під його управлінням, умінь виконувати його налагодження і адаптацію до вирішення задач у наступній професійній діяльності чи повсякденному житті. Метою проведення лабораторних занять є розвиток у студентів навичок самостійного використання набутих знань, навичок та умінь і забезпечення засвоєння основних понять навчальної дисципліни.

Викладання навчального курсу супроводжується з використанням навчально-методичної літератури, перелік якої додається, виконанні розроблених завдань до лабораторних робіт, технічними засобами навчання, спеціальним програмним забезпеченням. В системі управління навчальними ресурсами MOODLE розміщено теоретичні відомості та завдання до лабораторних занять.

На консультаціях зі студентами передбачається з'ясування і обговорення проблемних питань, що стосуються виконання самостійних завдань до лекційних і лабораторних занять, незрозумілих студентами теоретичних питань тощо. Реалізація вищезгаданих вимог забезпечує один з головних напрямків професійної підготовки сучасного фахівця і дозволяє йому активно використовувати сучасні технології захисту даних під час розробки та тестування програмного забезпечення.

2. Інформаційний обсяг навчальної дисципліни

Зміст курсу «*Захист інформаційних ресурсів*» подано у вигляді модулів, до кожного з яких наведено перелік основних термінів та понять, що студенти повинні знати та основних вмінь, якими вони повинні оволодіти після вивчення відповідного модуля, а також тематику занять та анотації до них.

2.1. Структура навчальної дисципліни

Змістовий модуль 1. Апаратно-програмні засоби захисту даних в комп'ютерних системах.

Тема 1. Основні поняття з галузі захисту інформаційних ресурсів.

Зміст теми: Актуальність проблеми комп'ютерної безпеки, цілісність даних, конфіденційність даних, доступність даних, розголошення даних, витік даних, захист даних, порушенням режиму доступу, несанкціонований доступ, об'єкт злочину, блокування даних, модифікація даних, одержання захищуваних даних, фільтрація даних, канал витоку даних, помилка, прорахунок, вразливість інформаційної системи, види загроз, джерела загроз, контроль безпеки, види атак, вторгнення, політика безпеки, класифікація навмисних загроз безпеки комп'ютерних систем.

Тема 2. Засоби парольної ідентифікації та адміністрування.

Зміст теми: Ідентифікація, засоби парольної ідентифікації в операційних системах, в програмних додатках, в мережевих сервісах, способи захисту від перебирання паролів, варіанти заміни традиційних паролів, способи створення складних паролів.

Тема 3. Архівування та резервне копіювання даних.

Зміст теми: Стискування, архівація даних, архіватор, ступінь стискування, коефіцієнт стискування, методи стискування файлів, резервне копіювання, технології резервного копіювання.

Тема 4. Захист вмісту зовнішньої пам'яті.

Зміст теми: Перспективні розробки у сфері зберігання вмісту запам'ятовуючих пристроїв, технології захисту оптичних дисків від несанкціонованого копіювання, діагностика та профілактика жорстких магнітних дисків, технології захисту флеш-накопичувачів, засоби відновлення пошкодженого і втраченого вмісту запам'ятовуючих пристроїв, гарантоване вилучення вмісту запам'ятовуючих пристроїв.

Тема 5. Захист програмного забезпечення.

Зміст теми: Вразливості програмного забезпечення та засоби боротьби з ними, дослідження вихідних текстів програмного забезпечення, захист програм встановлених на жорсткому диску, захист програм від вивчення.

Тема 6. Захист вмісту запам'ятовуючих пристроїв від шкідливих програм.

Зміст теми: Комп'ютерні віруси і засоби боротьби з ними, історія комп'ютерних вірусів, класифікація комп'ютерних вірусів, антивірусні програми, типи антивірусних програм, методи

розпізнавання шкідливих об'єктів, захист комп'ютера від шпигунських програм.

Тема 7. *Поширені види мережевих атак і способи захисту від них.*

Зміст теми: Мережеві атаки, види мережевих атак, сегментація мереж, міжмережеві екрани, списки управління доступом (ACL), загрози використання глобальної мережі Інтернет, методи захисту.

Тема 8. *Організація бездротового зв'язку, специфічні атаки на бездротові мережі та способи захисту від них.*

Зміст теми: Актуальні проблеми використання безпроводних мереж, типи загроз безпеці в безпроводних мережах, способи захисту даних в безпроводних мережах.

Змістовий модуль 2. Криптографічні та стеганографічні методи захисту даних.

Тема 9. *Основні поняття криптографії. Коротка історія криптографії. Основні поняття стеганографії. Історія стеганографії. Стеганографічні методи і системи.*

Зміст теми: Поняття криптології, криптографії. Ключ, шифрування, зашифровування, розшифровування, криптостійкість, криптоаналіз, методи криптоаналізу, криптографічні методи захисту даних. Поняття стеганографії, історія стеганографії, стеганографічні методи і системи.

Тема 10. *Популярні алгоритми шифрування даних.*

Зміст теми: Алгоритми шифрування, асиметричні криптографічні алгоритми, симетричні криптографічні алгоритми.

2.2. Темы лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Засоби парольної ідентифікації та адміністрування.	2
2	Архівування та резервне копіювання даних.	2
3	Захист вмісту зовнішньої пам'яті.	2
4	Захист програмного забезпечення.	2
5	Захист даних від шкідливих програм.	2
6	Поширені види мережевих атак і способи захисту від них.	2
7	Криптографічні та стеганографічні програмні засоби..	2

2.3. Самостійна (індивідуальна) робота

Перелік тем, винесених на самостійне опрацювання

№ Самос- тійної роботи	Теми	Бали
1	<ul style="list-style-type: none"> • Концепція інформаційної безпеки: стратегія і тактика. • Інформаційна безпека: поняття, сутність та значення. • Аудит інформаційної безпеки. • Інформаційна безпека в аспекті соціальної діяльності. • Організаційно-управлінські заходи забезпечення інформаційної безпеки. 	8
2	<ul style="list-style-type: none"> • Електронний бізнес та інформаційна безпека. • Співвідношення категорій «інформаційна безпека» та «захист даних». • Інформатизація її вплив на інформаційну безпеку. • Принципи організації інформаційної безпеки та захисту даних. • Визначення критеріїв та аналіз оперативного стану інформаційної безпеки. 	8
3	<ul style="list-style-type: none"> • Захист даних в соціальних мережевих сервісах. • Класифікація злочинів у сфері інформаційних правовідносин. • Комп'ютерні злочини та захист даних. • Комп'ютерна злочинність та комп'ютерна безпека. • Виявлення та розслідування комп'ютерних злочинів. • Протидія комп'ютерним злочинам. • Інженерно-технічний захист даних: сутність та загальна характеристика. • Фізичні засоби захисту даних. • Апаратні засоби захисту даних. • Програмні засоби захисту даних. 	8

	<ul style="list-style-type: none"> • Технічні канали витоку даних. • Інженерно-технічні заходи забезпечення інформаційної безпеки. • Програмно-апаратний захист даних. • Програмно-апаратні засоби шифрування даних. • Організаційно-технічні (інженерно-технологічні) заходи забезпечення інформаційної безпеки. • Поняття та сутність організації технічного захисту даних в автоматизованих системах. • Організація інформаційної безпеки інженерно-технічними засобами. • Способи несанкціонованого доступу технічними засобами до інформаційних систем та їх класифікація. 	
	Всього	24

Методичні рекомендації до написання реферату

Реферат (лат. *referre* - доповідати, повідомляти) підводить підсумок вивчення студентами як окремої теми (самостійна робота), так і дисципліни в цілому.

Обсяг реферату визначається специфікою досліджуваного питання і змістом матеріалів (документів), їх науковою цінністю та практичним значенням. Оптимальний обсяг реферату складає 10-15 сторінок. **Реферат має відповідати вимогам до оформлення рукопису кваліфікаційної роботи:** *вступ і висновки в сумі не повинні перевищувати 20% від її загального обсягу; текст друкується через 1,5 інтервали на одній сторінці стандартного аркуша з такими полями: ліве - 30 мм, праве - 15 мм, верхнє - 20 мм, нижнє - 20 мм; всі сторінки нумеруються: загальна нумерація починається з титульного листа, проте порядковий номер на ньому не ставиться.*

На титульному листі реферату вказуються: *офіційна назва закладу освіти, інституту (факультету) і кафедри; прізвище та ініціали автора реферату (абревіатура навчальної групи); повна назва теми; прізвище та ініціали наукового керівника, його науковий ступінь і вчене звання; місто, де знаходиться навчальний заклад та рік написання реферату.*

Після титульного листа подається зміст реферату з точною назвою кожного розділу (параграфу) і вказуванням його сторінок.

Список використаних джерел складається з дотриманням загально визнаних вимог до робіт, що готуються до друку. До списку використаних джерел мають бути включені лише безпосередньо використані в рефераті праці в алфавітному порядку авторів. Монографії і збірники, що не мають на титульному аркуші прізвища автора (авторів), включаються до загального списку за алфавітним розміщенням заголовку.

Тема реферату – це не просто повторення засвоєного матеріалу лекції або семінарського заняття. Вона повинна являти собою самостійне розроблення проблеми, достатньо чітко окресленої від інших. Неприпустиме поєднання декількох проблем або, навпаки, штучне виокремлення певної частини єдиного питання.

Важливими критеріями при доборі теми реферату, є її актуальність, широка джерельна база, наявність необхідного фактичного матеріалу, а також достатнє її висвітлення в науково-методичній літературі, що передбачає, в першу чергу, ознайомлення із загальною концепцією автора праці та його висновками.

Структура реферату:

- титульний аркуш;
- зміст (план);
- вступ;
- розділи (вони часто поділяються на параграфи);
- висновки;
- список використаних джерел;
- додатки (у яких наводяться таблиці, схеми, діаграми тощо);
- перелік умовних позначень.

У вступі реферату обґрунтовується актуальність теми, її особливості, значущість з огляду на розвиток науки та практики або науково-методичної діяльності у сфері освіти. У вступі необхідно подати аналіз використаних джерел, назвавши при цьому авторів, які вивчали дану тематику, визначити сутність основних чинників, що вплинули та розвиток явища або процесу, що досліджується, на недостатньо досліджені питання, з'ясувавши причини їх слабкої аргументації.

Основну частину реферату складають кілька розділів (що

можуть бути розбиті на параграфи), логічно поєднані між собою.

Виклад матеріалу в рефераті має бути логічним, послідовним, без повторень. Слід використовувати синтаксичні конструкції, характерні для стилю наукових документів, уникати складних граматичних зворотів, незвичних термінів і символів або пояснювати їх відразу, при першому згадуванні в тексті реферату. Терміни, окремі слова і словосполучення можна замінювати абрєвіатурами і сприйнятливими текстовими скороченнями, значення яких зрозумілі з контексту реферату.

Неприпустимо використовувати цитати без посилання на автора. При цитуванні будь-якого фрагменту джерела недопустимі неточності. Взагалі, цитатами не слід зловживати. Якщо якийсь важливий документ потребує наведення його в тексті реферату в повному обсязі, то краще винести його в додатки.

У рефераті необхідно визначити і викласти основні тенденції дослідження, підтвердити їх найтипівішими прикладами, відобразити сучасні ідеї та гіпотези, методики та методичні підходи до вивчення проблеми. Доцільно зупинитися на якомусь дискусійному моменті і спробувати проаналізувати позиції сторін, приєднавшись до однієї з них, чи висловити власну думку на певну проблему та визначити перспективи її вирішення.

Кожен розділ реферату повинен завершуватись короткими висновками, чіткими і лаконічними, де узагальнено оцінки та практичні рекомендації. Можна стисло вказати на перспективи подальшого дослідження даної проблеми.

Реферат оцінюється за такими критеріями: *актуальність; наукова та практична цінність; глибина розкриття теми, вирішення поставлених завдань; повнота використання рекомендованої літератури; обґрунтування висновків; грамотність; стиль викладу; оформлення реферату; обсяг виконаної роботи; завершеність дослідження.*

2.4. Методичне забезпечення

- Навчальна типова програма дисципліни.
- Робоча програма дисципліни.
- Плани занять.
- Навчальні-наочні посібники, технічні засоби навчання тощо.

- Конспект лекцій з дисципліни.
- Комплексні контрольні роботи (ККР) для визначення залишкових знань з дисципліни.
- Інструктивно-методичні матеріали лабораторних занять.
- Контрольні завдання до лабораторних занять.
- Методичні рекомендації та розробки викладача.
- Методичні матеріали, що забезпечують самостійну роботу студентів.
- Навчально-методична карта дисципліни:

Схема організації навчального процесу

Тиждень	Лекції	Бали	Лабораторні (практичні, семінарські) заняття, індивідуальні завдання, модульний контроль	Бали	Самостійна (індивідуальна) робота	Бали
Модуль 1. Апаратно-програмні засоби захисту даних в комп'ютерних системах						
1	Л.№1. Вступ. Основні поняття з галузі захисту інформаційних ресурсів. Класифікація загроз безпеки комп'ютерних систем. Засоби пароліної ідентифікації та адміністрування.	5				
2			Л.Р.№1. Засоби пароліної ідентифікації та адміністрування.	10	С.Р.№1	8
3	Л.№2. Архівування та резервне копіювання даних. Захист вмісту зовнішньої пам'яті.	5	Л.Р.№2. Архівування та резервне копіювання даних.	10		
4			Л.Р.№3. Захист вмісту зовнішньої пам'яті.	10	С.Р. №2	8
5	Л.№3. Захист програмного забезпечення. Захист вмісту запам'ятовуючих пристроїв від шкідливих програм. Поширені види мережевих атак і способи захисту від них.	5	Л.Р.№4. Захист програмного забезпечення.	10		
6			Л.Р.№5 Захист даних від шкідливих програм.	10		
7			Л.Р.№6. Поширені види мережевих атак і способи захисту від них. Модульний контроль №1.	10 10		
Всього:		15	Всього:	70	Всього:	16
Всього за I модуль:						101

Модуль 2. Криптографічні та стеганографічні методи захисту даних					
8	Л.№4. Основні поняття криптографії. Коротка історія криптографії. Основні поняття стеганографії. Історія стеганографії. Стеганографічні методи і системи.	5	Л.Р.№7. Криптографічні та стеганографічні програмні засоби. Модульний контроль №2.	10 10	С.Р. №3 8
9	Л.№5. Популярні алгоритми шифрування даних.	5			
Всього:		10	Всього:	20	Всього: 8
Всього за II модуль:					38
Всього за лекції		25	Всього за лабораторні (практичні, семінарські) заняття	90	Всього за самостійну роботу 24
Всього за семестр					139
Всього за лекції (100)		18	Всього за лабораторні (практичні, семінарські) заняття (100)	65	Всього за самостійну роботу (100) 17
Всього за семестр (100)					100
Залік					100
Оцінка за курс (середній бал)					100

Пояснення до схеми

1. Оцінювання лекційних занять:

№	Критерії	Бали
1	За відвідування.	2
2	За наявність конспекту лекції (Тести).	3
Всього:		5

Примітка: Перевірка записів конспекту здійснюється викладачем на останній лекції, в кінці кожного модуля або на останній лекції, в кінці семестру. Також може бути у формі тестових завдань.

2. Оцінювання лабораторних (практичних, семінарських) занять:

№	Критерії	Бали
1	За відвідування.	2
2	За теоретичні знання.	4
3	За виконання практичних завдань.	4
Всього:		10

Примітка: Захист лабораторних (практичних, семінарських) робіт здійснюється тільки на лабораторних (практичних, семінарських) заняттях згідно схеми організації навчального процесу.

3. Оцінювання самостійної (індивідуальної) роботи:

№	Критерії	Бали
1	За реферат.	4
2	За презентацію.	2
3	За виступ.	2
Всього:		8

Примітка: Потрібно опрацювати протягом семестру, як мінімум, 1 із тем, які винесені на самостійне опрацювання, і скласти її (їх) не пізніше завершення відповідного модуля згідно схеми організації навчального процесу. Додаткові бали за самостійну роботу також можна отримати на лекційних та на лабораторних (практичних, семінарських) заняттях за активність при обговоренні навчального матеріалу.

Консультації проводяться на лекційних, лабораторних (практичних, семінарських) заняттях.

3. Рекомендована література

Основна:

1. Баричев С.Т., Гончаров В.В., Серов Р.Е. Основы современной криптографии. М.: Горячая линия-Телеком, 2001. — 152 с.
2. Блэк У. Интернет: протоколы безопасности. Учебный курс. — СПб.: Питер, 2010 — 288 с.
3. Болотов А.А., Гашков А.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. — М.: КомКнига, 2006. — 328 с.
4. Бормотов С.В. Системное администрирование на 100 % (+CD). — СПб.: Питер, 2006. — 256 с.
5. Варфоломеев А.А., Жуков А.Е., Пудовкина М.А. Поточные криптосистемы. Основные свойства и методы анализа стойкости. — М.: ПАИМС, 2000. — 36 с.
6. Жельников В. Криптография от папируса до компьютера. — М.: АБФ, 1996. — 130 с.
7. Зубов А.Ю. Совершенные шифры. — М.: Гелиос АРВ, 2003. — 160 с.
8. Касперски К. Восстановление данных. Практическое руководство: Пер. с англ. — СПб.: БХВ-Петербург, 2006. — 352 с.
9. Касперски К., Рокко Е. Искусство дизассемблирования. Наиболее полное руководство в подлиннике. — СПб: БХВ-Петербург, 2008. — 891 с.

10. Курило А.П., Зефиров С.Л., Голованов В.Б. и др. Аудит информационной безопасности. — М.: Издательская группа "БДЦ-пресс", 2006. — 304 с.
11. Митник К. Искусство вторжения: Пер. с англ. Семенова А.В. — М.: АйТи, ДМК Пресс, 2005. — 280 с.
12. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. — СПб.: Лань, 2000. — 256 с.
13. Нечаев В.И. Элементы криптографии (Основы теории защиты информации). — М.: Высшая школа, 1999. — 200 с.
14. Низамутдинов М.Ф. Тактика защиты и нападения на Web-приложения. — СПб.: БХВ-Петербург, 2005. — 432 с.
15. Норткат С, Новак Дж. Обнаружение нарушений безопасности в сетях. — М.: Издательский дом "Вильяме", 2003. — 448 с.
16. Оглтри Т. Firewalls. Практическое применение межсетевых экранов. — М. ДМК пресс, 2001. — 400 с.
17. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. — М: ДМК, 2000. — 448 с.
18. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для студ. высш. учеб. заведений / В.В. Платонов. — М. : Издательский центр "Академия", 2006. — 240 с.
19. Практическая криптография: алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади. — М.: СОЛОН-Пресс, 2002. — 256 с.
20. Скляр Д. Искусство защиты и взлома информации. — СПб.: БХВ-Петербург, 2004. — 288 с.
21. Смалько О.А. Захист інформаційних ресурсів: Монографія. - Кам'янець-Подільський: ПП Буйницький О А, 2011. - 704 с
22. Фленов М.Е. РНР глазами хакера. — СПб.: БХВ-Петербург, 2005. — 304 с.
23. Форд Дж. Ли. Персональная защита от хакеров. Руководство для начинающих. Пер. с англ. — М.: КУДИЦ-ОБРАЗ, 2002. — 272 с.
24. Фостер Дж., Лю В. Разработка средств безопасности и эксплойтов. — М.: Издательство "Русская Редакция"; СПб.: Питер, 2007. — 432 с.
25. Хоффман Л.Дж. Современные методы защиты информации. — М.: Сов. Радио, 1980. — 246 с.
26. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. — СПб.: Питер, 2003. — 368 с.

27. Щербakov Л.Ю., Домашев А.В. Прикладная криптография. Использование и синтез криптографических интерфейсов. – М: Издательско-торговый дом "Русская Редакция", 2003. – 416 с.
Додаткова:
28. Громов В.И. Васильев Г.А. Энциклопедия компьютерной безопасности. — Режим доступа: <http://kiev-security.org.ua/b/1.shtml>. — Название с экрана.
29. Зиммерман Филипп. Кодирование с открытым ключом для всех. Руководство пользователя PGP. — Режим доступа: <http://lib.metromir.ru/book2571>. — Название с экрана.
30. Иллюстрированный самоучитель по защите информации. — Режим доступа: <http://www.inattack.ru/program/525.html>. — Название с экрана.
31. Иллюстрированный самоучитель по теории операционных систем. — Режим доступа: <http://www.soft-info.ru/downloads/1230999291>. — Название с экрана.
32. Руководство по информационной безопасности. — Режим доступа: http://unix1.jinr.ru/faq_guide/security/jet/secplant. — Название с экрана.
33. Стандарты и спецификации в области информационной безопасности. Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт. Режим доступа: <http://www.intuit.ru/department/security/secbasics/5>. — Название с экрана.
34. Техника восстановления данных с лазерных дисков или практическое знакомство с сессиями. — Режим доступа: <http://hack-tools.ucoz.com>. — Название с экрана.
35. Ферри Д. Секреты супер-хакера. — Режим доступа: <http://www.domknig.net/book-2697.html>. — Название с экрана.
- Інформаційні ресурси:*
36. <http://www.moodle.fi.npu.edu.ua/course/view.php?id=424>.
37. <http://www.moodle.fi.npu.edu.ua/course/view.php?id=425>.

4. Форма підсумкового контролю успішності навчання

Залік є формою підсумкового контролю результатів навчання студентів і має на меті перевірку системності засвоєння програмового матеріалу, цілісності бачення навчального курсу, рівня осмислення

знань та набуття умінь, їх комплексного застосування у практичній діяльності, діагностування ефективності самостійної навчальної роботи студентів.

Відмітка «зараховано» виставляється студенту за умови набору більше 60 рейтингових балів, а саме:

- регулярного відвідування лекційних і лабораторних занять або їх негайного відпрацювання, своєчасного складання усіх видів поточного контролю з позитивними результатами;
- поглибленні набутих знань у процесі самостійної роботи;
- засвоєнні змісту навчального курсу в обсязі, передбаченому галузевим стандартом вищої освіти.

Якщо студент з поважних причин, що підтверджено документально, був відсутній на заняттях, він має право на одне перескладання з можливістю отримання максимальної кількості балів. Термін перескладання визначається викладачем.

Якщо впродовж семестру студент пропустив значну кількість занять, не має оцінок за виконання модулів, у відповідних графах «Відомості обліку успішності» виставляються «0», у графі «залік» виставляється «не зараховано». Якщо студент з поважних причин, що підтверджено документально, був відсутній на заняттях, він має право на одне перескладання з можливістю отримання максимальної кількості балів. Термін перескладання визначається викладачем.

Рейтинговий регламент Факультету. Шкала відповідності

За шкалою ECTS	За шкалою університету	Визначення	Оцінка за національною шкалою	
			Екзамен	Залік
A	90 – 100	Відмінно	5 (відмінно)	Зараховано
B	80 – 89	Дуже добре	4 (добре)	
C	70 – 79	Добре		
D	65 – 69	Задовільно	3 (задовільно)	
E	60 – 64	Достатньо		
FX	35 – 59	Незадовільно можливістю повторного складання	2 (незадовільно)	Не зараховано
F	1 – 34	Незадовільно обов'язковим повторним курсом		

5. Засоби діагностики успішності навчання

Видом контролю навчальних досягнень студентів під час вивчення курсу є залік. За результатами роботи на лабораторних заняттях, виконання завдань для самостійного опрацювання, підготовки та виступу з доповіддю на заняттях, модульних тестів, студенти накопичують певну кількість балів, відповідно до якої відбувається оцінювання їх навчальних досягнень.

Побудова програми за блочно-модульною схемою спрямована на максимальну індивідуалізацію процесу навчання. Структура програми дібрана так, щоб надати студентам можливість навчатись в індивідуальному темпі та орієнтуватись на певні рівні вимог щодо засвоєння навчального матеріалу.

Контроль знань студентів здійснюється за модульно-рейтинговою системою. Навчальна діяльність студентів впродовж семестру оцінюються за 100-бальною системою. Робота в семестрі поділяється на змістові модулі.

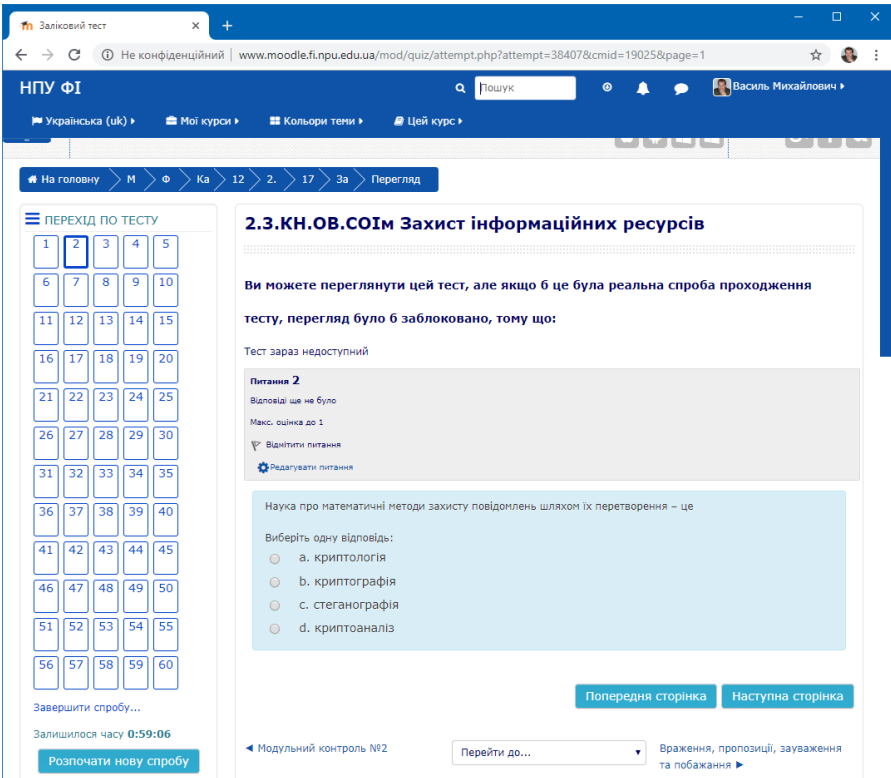
Накопичення балів протягом семестру відбувається так:

№ з/п	Вид діяльності	Кількість балів за дидактичну одиницю	Кількість лекцій, практичних робіт тощо	Загальна кількість балів
1	Виконання завдань на лабораторних заняттях	10	14+2	160
2	Відвідування та активність під час лекцій	5	15	75
3	Індивідуальна робота та презентація власних досліджень (самостійна робота)	8	5	40
Загальна кількість балів (поточна успішність)				139
Формула переведення балів у бали за модульно-рейтинговою системою $100 \cdot A / 139$, де А – кількість набраних студентом балів				100
Залік				100
Оцінка за курс (середній бал)				100

Засоби діагностики успішності навчання:

- теоретичні запитання та практичні завдання до лабораторних робіт;
- комплекс тестових завдань для модульного (підсумкового) контролю рівня навчальних досягнень студентів;
- індивідуальні завдання студентам;
- комплексна контрольна робота.

Залік проводиться у формі комп'ютерного тестування, де потрібно відповісти на 60 тестових завдання закритої форми (див.Рис. 1)



The screenshot shows a Moodle quiz page titled "Заліковий тест" (Final Test). The browser address bar shows the URL: www.moodle.fi.npu.edu.ua/mod/quiz/attempt.php?attempt=38407&cmid=19025&page=1. The page header includes "НПУ ФІ" and a search bar. The main content area is titled "2.3.КН.ОВ.СОІм Захист інформаційних ресурсів". A message states: "Ви можете переглянути цей тест, але якщо б це була реальна спроба проходження тесту, перегляд було б заблоковано, тому що: Тест зараз недоступний". Below this, "Питання 2" is displayed with the text: "Наука про математичні методи захисту повідомлень шляхом їх перетворення – це". The question asks to select one answer from four options: a. криптологія, b. криптографія, c. стеганографія, d. криптоаналіз. The interface includes a grid of 60 question numbers (1-60) on the left, a "Залишилося часу 0:59:06" timer, and navigation buttons like "Попередня сторінка" and "Наступна сторінка".

Рис. 1. Тестове завдання закритої форми

ДЛЯ ЗАМІТОК