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

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ

ПРОГРАМА

навчальної дисципліни

підготовки **бакалавра**

галузь знань **0403 Системні науки та кібернетика**

напряму підготовки **6.040302 Інформатика***

КИЇВ – 2015

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

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ

ПРОГРАМА

навчальної дисципліни

підготовки **бакалавра**

галузь знань **0403 Системні науки та кібернетика**

напряму підготовки **6.040302 Інформатика***

КИЇВ – 2015

УДК 004.056.5(073)
ББК 32.97я73
338

Рекомендовано до друку Вченою радою Інституту інформатики Національного педагогічного університету імені М.П. Драгоманова (протокол № 6 від 26 грудня 2012 р.).

Рекомендовано до друку Науково-методичною радою Національного педагогічного університету імені М.П. Драгоманова (протокол № 3 від 20 грудня 2012 р.).

Рецензенти:

Дем'яненко В.М. — кандидат педагогічних наук, доцент, заступник директора Інституту інформаційних технологій та засобів навчання АПН України;

Струтинська О.В. — кандидат педагогічних наук, доцент кафедри теоретичних основ інформатики інституту інформатики НПУ імені М.П. Драгоманова;

338 Захист інформаційних ресурсів: програма навчальної дисципліни для підготовки студентів напрямку 6.040302 «Інформатика*» Інституту інформатики НПУ імені М.П. Драгоманова / укл. В.М. Франчук (в авторській редакції). - Київ: Вид-во НПУ імені М.П. Драгоманова, 2015 р. – 21 с.

В програмі наведено зміст навчальної дисципліни «Захист інформаційних ресурсів» для підготовки студентів напрямку 6.040302 «Інформатика*» Інституту 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 вищих педагогічних навчальних закладів.

УДК 004.056.5(073)
ББК 32.97я73
© В.М. Франчук, 2015
© НПУ імені М.П. Драгоманова, 2015

ЗМІСТ

ВСТУП

Програма вивчення варіативної навчальної дисципліни (за вибором університету) «Захист інформаційних ресурсів» складена відповідно до освітньо-професійної програми підготовки бакалавра напряму підготовки ***6.040302 Інформатика**** і є основним документом, в якому визначається обсяг і орієнтовний порядок вивчення змістових модулів навчальної дисципліни відповідно до галузевого стандарту вищої освіти.

Предметом вивчення навчальної дисципліни є процес формування у майбутніх вчителів інформатики умінь захисту інформаційних ресурсів.

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 «Вступ до інформатики», «Інформаційно-комунікаційні технології», «Комп'ютерні мережі та Інтернет», «Програмування», «Архітектура комп'ютера та конфігурування комп'ютерних систем» і мають базові знання про склад і призначення основних компонентів обчислювальної техніки. Вивчення даного курсу забезпечує необхідний рівень знань для опанування дисциплінами «Спеціальний лабораторний практикум з інформатики», «Вибрані питання інформатики», «Створення та адміністрування дистанційних освітніх ресурсів», «Сучасні інформаційні технології в освіті».

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

- Основні поняття захисту інформаційних ресурсів. Апаратно-програмні засоби захисту даних в комп'ютерних системах.
- Криптографічні та стеганографічні методи захисту даних.

Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання

<table>
<tr><td rowspan="2">Кількість кредитів – 4,5</td><td>Галузь знань
0403 Системні науки та кібернетика
(шифр і назва)</td><td colspan="2" rowspan="2">Варіативна
(за вибором студента)</td></tr>
<tr><td>Напрям підготовки
6.040302 Інформатика*
(шифр і назва)</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">Спеціальність (професійне спрямування):
6.040302 Інформатика*</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 2</td><td>2-й (3-й)</td><td>3-й</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання реферат</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 162</td><td>4-й (6-й)</td><td>5-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="11">Тижневих годин для денної форми навчання:
аудиторних – 4
в т.ч. індивідуальна робота,
самостійної роботи студента – 9,5</td><td rowspan="11">Освітньо-кваліфікаційний рівень:
бакалавр</td><td>36 год.</td><td>10 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>0 год.</td><td>0 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>36 год.</td><td>10 год.</td></tr>
<tr><td colspan="2">Індивідуальна робота</td></tr>
<tr><td>8 год.
(0 год.)</td><td>0 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>82год.
(90 год.)</td><td>142 год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання:
0 год.</td></tr>
<tr><td colspan="2">Вид контролю: екзамен</td></tr>
</table>

Примітка.

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить:

- для денної форми навчання – 0,98;
- для заочної форми навчання – 0,14.

Примітка: в дужках «( )» позначено відомості для освітньо-кваліфікаційного рівня бакалавра на базі диплому молодшого спеціаліста.

1. Мета та завдання навчальної дисципліни

Метою вивчення дисципліни «Захист інформаційних ресурсів» є навчання студентів напрямку підготовки ***6.040302 Інформатика**** до свідомого, активного та вмілого використання нових інформаційних технологій у навчально-виховному процесі.

Основними завданнями вивчення дисципліни «Захист інформаційних ресурсів» є**:**

- розкрити місце і значення дисципліни в загальній і професійній освіті;
- з'ясувати психолого-педагогічні аспекти засвоєння предмету, взаємозв'язки курсу з іншими навчальними дисциплінами, зокрема з інформатичними дисциплінами;
- навчити студентів ефективно захищати під час навчально-виховного процесу інформаційні ресурси;
- навчити майбутніх фахівців орієнтуватися у засобах захисту навчальних комп'ютерних систем, свідомо обирати тип, склад та конфігурацію обчислювальної техніки у відповідності до конкретних вимог навчального процесу, психофізіологічних особливостей учнів;
- Продемонструвати ефективність використання методів захисту інформаційних ресурсів при організації навчального процесу.
- Розглянути криптографічні та стеганографічні методи захисту даних.

Згідно з вимогами освітньо-професійної програми студенти повинні:

знати:

- можливі дії зловмисника або некомпетентного користувача, направлені на порушення безпеки даних;
- найуразливіші для атак зловмисником чи некоректних дій некомпетентного користувача елементи комп'ютерних систем;
- механізми розв'язування типових проблем захисту даних;

вміти:

- аналізувати механізми реалізації методів захисту конкретних об'єктів і процесів для розв'язування професійних задач;
- застосовувати засоби захисту і спеціалізовані програмні продукти для розв'язування типових проблем в галузі захисту інформаційних ресурсів;

- кваліфіковано оцінювати можливості застосування конкретних механізмів захисту;
- компетентно використовувати апаратні засоби захисту при розв'язуванні практичних задач.

що забезпечують формування таких компетенцій:

- соціально-особистісних;
- загальнонаукових;
- інструментальних;
- професійних.

На вивчення курсу «Захист інформаційних ресурсів», який вивчається на ІІ курсі у 4 семестрі, відводиться 4,5 кредити або 162 навчальні години, з яких 82 годин відведено на самостійну навчально-пізнавальну роботу студентів, а 80 години – на аудиторні заняття, які проводяться у формі лекційних занять (36 год.), лабораторних робіт (36 год.) та індивідуальної роботи (8 год.).

Назва дисципліни	Вид контролю	ECTS	Всього	Самостійна робота	Аудиторні	Лекції	Лабораторні	Індивідуальна робота
Захист інформаційних ресурсів	Залік (4 сем.)	4,5	162	82	80	36	36	8

2. Інформаційний обсяг навчальної дисципліни

Змістовий модуль 1. Основні поняття захисту інформаційних ресурсів. Апаратно-програмні засоби захисту даних в комп'ютерних системах.

Тема 1. Основні поняття з галузі захисту інформаційних ресурсів.

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.

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.

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

Тема 4. Захист вмісту зовнішньої пам'яті.

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.

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.

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.

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.

Актуальні проблеми використання безпровідних мереж, типи загроз безпеці в безпровідних мережах, способи захисту даних в безпровідних мережах.

Змістовий модуль 2. Криптографічні та стеганографічні методи захисту даних.

Тема 9. Основні поняття криптографії. Коротка історія криптографії.

Поняття криптології, криптографії. Ключ, шифрування, зашифровування, розшифровування, криптостійкість, криптоаналіз, методи криптоаналізу, криптографічні методи захисту даних.

Тема 10. Популярні алгоритми шифрування даних.

Алгоритми шифрування, асиметричні криптографічні алгоритми, симетричні криптографічні алгоритми.

Тема 11. Використання електронного підпису.

Криптосистеми з відкритим ключем, електронний (цифровий) підпис, Технології застосування систем електронного цифрового підпису, генерація ключів.

Тема 12. Програмно-апаратні засоби шифрування даних.

Реалізації криптозахисту на апаратному рівні. Архітектура апаратних засобів криптозахисту. Організація інтерфейсу для роботи з прикладними програмами.

Тема 13. Основні поняття стеганографії. Історія стеганографії. Стеганографічні методи і системи.

Поняття стеганографії, історія стеганографії, стеганографічні методи і системи.

Тема 14. Деякі проблеми і перспективи використання криптографічних засобів захисту даних.

Проблеми шифрування великих повідомлень, сучасні способи вирішення проблеми розподілу ключів, системи біометричної аутентифікації, перспективи використання криптографічних засобів захисту даних.

2.1. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна і вечірня форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Модуль 1												
Змістовий модуль 1. ***Основні поняття захисту інформаційних ресурсів. Апаратно-програмні засоби захисту даних в комп'ютерних системах.***												
Тема 1. Основні поняття з галузі захисту інформаційних ресурсів.	9	2		2		5	9.2	0.6		0.6		8
Тема 2. Засоби парольної ідентифікації та адміністрування.	9	2		2		5	9.2	0.6		0.6		8
Тема 3. Архівування та резервне копіювання даних.	9	2		2		5	9.2	0.6		0.6		8
Тема 4. Захист вмісту зовніньої пам'яті.	9	2		2		5	9.2	0.6		0.6		8
Тема 5. Захист програмного за-	10	2		2		5	9.2	0.6		0.6		8

безпечення.												
Тема 6. Захист вмісту запам'ято-вуючих пристроїв від шкідливих програм.	10	2		2		5	9	0.5		0.5		8
Тема 7. Поширені види мережевих атак і способи захисту від них.	10	2		2		5	9	0.5		0.5		8
Тема 8. Організація бездрото-вого зв'язку, специфічні атаки на бездротові мережі та способи захисту від них.	14 (10)	2		2	4	5	9	0.5		0.5		8
Разом за змістовим модулем 1	80	16		16	4	41	81	5		5		71
Змістовий модуль 2. ***Криптографічні та стеганографічні методи захисту даних.***												
Тема 9. Основні поняття криптогра-фії. Коротка історія криптогра-	10	2		2		6	9.2	0.6		0.6		8

фії.												
Тема 10. Популярні алгоритми шифрування даних.	26	10		10		6	9.2	0.6		0.6		8
Тема 11. Використання електронного підпису.	10	2		2		6	9.2	0.6		0.6		8
Тема 12. Програмно-апаратні засоби шифрування даних.	10	2		2		6	9.2	0.6		0.6		8
Тема 13. Основні поняття стеганографії. Історія стеганографії. Стеганографічні методи і системи.	10	2		2		6	9.2	0.6		0.6		8
Тема 14. Деякі проблеми і перспективи використання криптографічних засобів захисту даних.	12	2		2		8	9	0.5		0.5		8
Разом за	82	20		20	4	38	81	5		5		71

змістовим модулем 2												
Усього годин	162	36		36	8	82	162	10		10		142

2.2. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Налагодження та використання віртуальних комп'ютерів.	2
2	Засоби парольної ідентифікації та адміністрування.	2
3	Архівування та резервне копіювання даних.	2
4	Захист вмісту зовнішньої пам'яті.	2
5	Захист програмного забезпечення.	2
6	Захист даних від шкідливих програм.	2
7	Поширені види мережевих атак і способи захисту від них.	2
8	Організація бездротового зв'язку, специфічні атаки на бездротові мережі та способи захисту від них.	2
9	Симетричні методи шифрування. Шифри Цезаря, Трітеміуса, Полібія.	2
10	Симетричні методи шифрування. Шифри Плейфера, «подвійний квадрат» Уітстона, Вернама.	2
11	Блокові криптографічні алгоритми. Шифри скітала («палиця»), стандартної та вертикальної перестановки.	2
12	Блокові криптографічні алгоритми. Шифри з використанням комбінованих перестановок, Шифри-трафарети. Квадрат та прямокутник Кардано.	2
13	Змішані симетричні криптосистеми. Багатоалфавітна криптосистема Віженера.	2
14	Асиметричні і гібридні криптосистеми.	2
15	Криптографічні та стеганографічні програмні засоби.	2

2.3. Самостійна (індивідуальна) робота

Перелік тем, винесених на самостійне опрацювання

№ Самостійної роботи	**Теми**	**Бали**

1	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	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	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.	8
4	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
5	Технічні канали витоку даних. Інженерно-технічні заходи забезпечення інформаційної безпеки. Програмно-апаратний захист 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.	8
	Всього	40

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 навчального закладу, 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 загальновизнаних 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 абревіатурами і сприйнятливими текстовими скороченнями, значення яких зрозуміле 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 найтиповішими 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

1. Навчальна типова програма дисципліни;
2. Робоча програма дисципліни;
3. Плани занять;
4. Навчальні-наочні посібники, технічні засоби навчання тощо;
5. Конспект лекцій з дисципліни;
6. Комплексні контрольні роботи (ККР) для визначення залишкових знань з дисципліни;
7. Інструктивно-методичні матеріали лабораторних занять;
8. Контрольні завдання до лабораторних занять.
9. Методичні рекомендації та розробки викладача;
10. Методичні матеріали, що забезпечують самостійну роботу студентів;
11. 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. Основні поняття захисту інформаційних ресурсів. Апаратно-програмні засоби захисту даних в комп'ютерних системах						

1	**Л.№1.** Вступ. Основні поняття з галузі захисту інформаційних ресурсів.	5	**Л.Р.№1.** Налагодження та використання віртуальних комп'ютерів.	10		
2	**Л.№2.** Класифікація загроз безпеки комп'ютерних систем.	5	**Л.Р.№2.** Засоби парольної ідентифікації та адміністрування.	10		
3	**Л.№3.** Засоби парольної ідентифікації та адміністрування.	5	**Л.Р.№3.** Архівування та резервне копіювання даних.	10		
4	**Л.№4.** Архівування та резервне копіювання даних.	5	**Л.Р.№4.** Захист вмісту зовнішньої пам'яті.	10	**С.Р.№1**	8
5	**Л.№5.** Захист вмісту зовнішньої пам'яті.	5	**Л.Р.№5.** Захист програмного забезпечення.	10		
6	**Л.№6.** Захист програмного забезпечення.	5	**Л.Р.№6.** Захист даних від шкідливих програм.	10		
7	**Л.№7.** Захист вмісту запам'ятовуючих пристроїв від шкідливих програм.	5	**Л.Р.№7.** Поширені види мережевих атак і способи захисту від них.	10		
8	**Л.№8.** Поширені види мережевих атак і способи захисту від них.	5	**Л.Р.№8.** Організація бездротового зв'язку, специфічні атаки на бездротові мережі та способи захисту від них.	10	**С.Р. №2**	8
9	**Л.№9.** Організація бездротового зв'язку, специфічні атаки на бездротові мережі та способи захисту від них.	5	**Модульний контроль №1.**	10		
Всього:		45	Всього:	90	Всього:	16
Всього за І модуль:						151
Модуль 2. Криптографічні та стеганографічні методи захисту даних						
10	**Л.№10.** Стан та перспективи використа-ння апаратно-програмних засобів захисту даних в комп'ютерних системах.	5	**Л.Р.№9.** Потокові криптогра-фічні алгоритми. (Шифри Цезаря, Трітеміуса, Полібія).	10	**С.Р. №3**	8
11	**Л.№11.** Основні поняття криптографії. Коротка історія криптографії.	5	Л.Р.№10. Потокові криптогра-фічні алгоритми. (Шифри Плейфера, «подвійний квадрат» Уітстона, Вернама).	10		
12	**Л.№12.** Популярні алгоритми шифрування даних (симетричні: потокові).	5	**Л.Р.№11.** Блокові криптогра-фічні алгоритми. (Шифри скітала («палиця»), стандартної та вертикальної перестановки).	10		
13	**Л.№13.** Популярні алгоритми шифрування даних (симетричні: блокові).	5	**Л.Р.№12.** Блокові криптогра-фічні алгоритми. (Шифри з використанням комбінованих перестановок, Шифри-трафарети. Квадрат та прямокутник	10	**С.Р. №4**	8

			Кардано).			
14	**Л.№14.** Популярні алгоритми шифрування даних (асиметричні).	5	**Л.Р.№13.** Змішані симетричні криптосистеми. (Багатоалфа-вітна криптосистема Віженера).	10		
15	**Л.№15.** Використання електронного підпису.	5	**Л.Р.№14.** Асиметричні і гібридні криптосистеми.	10		
16	**Л.№16.** Програмно-апаратні засоби шифрування даних.	5	**Л.Р.№15.** Криптографічні та стеганографічні програмні засоби.	10	**С.Р. №5**	8
17	**Л.№17.** Основні поняття стеганографії. Історія стеганографії. Стеганографічні методи і системи.	5	**Модульний контроль №2.**	10		
18	**Л.№18.** Стан та перспективи використання веб-орієнтованих навчальних комп'ютерних систем.	5	**Захист самостійних (індивідуальних) робіт. Залік.**			
Всього:		**45**	**Всього:**	**80**	**Всього:**	**24**
Всього за II модуль:						**149**
Всього за лекції		**90**	**Всього за лабораторні (практичні, семінарські) заняття**	**170**	**Всього за самостійну роботу**	**40**
Всього за семестр						**300**
Всього за лекції (100)		**30**	**Всього за лабораторні (практичні, семінарські) заняття (100)**	**57**	**Всього за самостій-ну роботу (100)**	**13**
Всього за семестр (100)						**100**

Пояснення до схеми

1. Оцінювання лекційних занять:

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

Примітка:

- Перевірка записів конспекту здійснюється викладачем на останній лекції, в кінці кожного модуля або на останній лекції, в кінці семестру.

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

1. Баричев СТ., Гончаров В.В., Серов Р.Е. Основы современной криптографии. М.: Горячая линия-Телеком, 2001. — 152 с.
2. Биячуев Т.А. Безопасность корпоративных сетей / под ред. Л.Г. Осовецкого. — СПб: СПб ГУ ИТМО, 2004. — 161 с.
3. Блэк У. Інтернет: протоколы безопасности. Учебный курс. — СПб.: Питер, 2010 — 288 с.
4. 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.
5. Бормотов СВ. Системное администрирование на 100 % (+CD). — СПб.: Питер, 2006. — 256 с.
6. Варфоломеев А.А., Жуков А.Е., Пудовкина М.А. Поточные криптосистемы. Основные свойства и методы анализа стойкости.

— М.: ПАИМС, 2000. — 36 с.
7. Гордейчик СВ., Дубровин В.В. Безопасность беспроводных сетей. — М.: Горячая линия-Телеком, 2008. — 288 с.
8. Жельников В. Криптография от папируса до компьютера. — М.: ABF, 1996. — 130 с.
9. Зубов А.Ю. Совершенные шифры. — М.: Гелиос АРВ, 2003. — 160 с.
10. Касперски К. Восстановление данных. Практическое руководство: Пер. с англ. — СПб.: БХВ-Петербург, 2006. — 352 с.
11. Касперски К., Рокко Е. Искусство дизассемблирования. Наиболее полное руководство в подлиннике. — СПб: БХВ-Петербург, 2008. — 891 с.
12. Курило А.П., Зефиров С.Л., Голованов В.Б. и др. Аудит информационной безопасности. — М.: Издательская группа "БДЦ-пресс", 2006. — 304 с.
13. Митник К. Искусство вторжения: Пер. с англ. Семенова А.В. — М.: АйТи, ДМК Пресс, 2005. —280 с.
14. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. — СПб.: Лань, 2000. — 256 с.
15. Нечаев В.И. Элементы криптографии (Основы теории защиты информации). — М.: Высшая школа, 1999. — 200 с.
16. Низамутдинов М.Ф. Тактика защиты н нападения на Web-приложения. — СПб.: БХВ-Петербург, 2005. — 432 с.
17. Норткат С, Новак Дж. Обнаружение нарушений безопасности в сетях. — М.: Издательский дом "Вильяме", 2003. — 448 с.
18. Оглтри Т. Firewalls. Практическое применение межсетевых экранов. — М. ДМК пресс, 2001. —400 с.
19. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. — М: ДМК, 2000. — 448 с.
20. 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.
21. Практическая криптографія: алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади. — М.: СОЛОН-Пресс, 2002. — 256 с.
22. Скляров Д. Искусство защиты и взлома информации. — СПБ.: БХВ-Петербург, 2004. — 288 с.
23. Смалько О.А. Захист інформаційних ресурсів: Монографія. -

Кам’янець-Подільський: ПП Буйницький О А, 2011. - 704 с
24. Фленов М.Е. PHP глазами хакера. — СПб.: БХВ-Петербург, 2005. — 304 с.
25. Форд Дж. Ли. Персональная защита от хакеров. Руководство для начинающих. Пер. с англ. — М.: КУДИЦ-ОБРАЗ, 2002. — 272 с.
26. Фостер Дж., Лю В. Разработка средств безопасности и эксплойтов. — М.: Издательство "Русская Редакция"; СПб.: Питер, 2007. — 432 с.
27. Хоффман Л.Дж. Современные методы защиты информации.— М.: Сов. Радио, 1980. — 246 с.
28. Чирилло Дж. Обнаружение хакерских атак. Для профессионалов. — СПб.: Питер. 2002. —864 с.
29. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. — СПб.: Питер, 2003. — 368 с.
30. Щербаков Л.Ю., Домашев А.В. Прикладная криптография. Использование и синтез криптографических интерфейсов. — М: Издательско-торговый дом "Русская Редакция", 2003. — 416 с.

Електронні ресурси та web-сайти

31. Громов В.И. Васильев Г.А. Энциклопедия компьютерной безопасности. — Режим доступа: http://kiev-security.org.ua/b/1.shtml. —Название с экрана.
32. Зиммерман Филипп. Кодирование с открытым ключом для всех. Руководство пользователя PGP. — Режим доступа: http://lib.metromir.ru/book2571. — Название с экрана.
33. Иллюстрированный самоучитель по защите информации. — Режим доступа: http://www.inattack.ru/program/525.html. — Название с экрана.
34. Иллюстрированный самоучитель по теории операционных систем. — Режим доступа: http://www.soft-info.ru/downloads/1230999291. — Название с экрана.
35. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака через Internet. — Режим доступа: http://www.rus-linux.net/lib.php?name=/MyLDP/BOOKS/books#lin-ru. — Название с экрана.
36. Наказ Міністерства транспорту та зв'язку України від 27.04.2005 "Про затвердження порядку проведення державної реєстрації електронних інформаційних ресурсів".— Режим доступу:

http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=z0528-05. — Назва з екрана.
37. Руководство по информационной безопасности. — Режим доступа: http://unix1.jinr.ru/ faq_guide/security/jet/secplant. — Название с экрана.
38. 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.
39. Техника восстановления данных с лазерных дисков или практическое знакомство с сессиями. — Режим доступа: http://hack-tools.ucoz.com. — Название с экрана.
40. Ферри Д. Секреты супер-хакера. — Режим доступа: http://www.domknig.net/book-2697.html. — Название с экрана.

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 при умові набору більше 60 рейтингових балів, а саме:

- регулярного відвідування лекційних і лабораторних занять або їх негайному відпрацюванні, 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 отриманн я 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» виставляється «1», у графі «залік» виставляється «не зараховано», а у графі «екзамен» – відмітка про не допуск до нього.

Рейтинговий регламент Інституту. 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 з можливістю повторного складання	2 (незадовільно)	Не зараховано
F	1 – 34	Незадовільно з 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 кредитно-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 протягом 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	2	3	4	5
1	Відвідування та активність під час лекцій	1	18	18
2	Виконання лабораторних робіт	2(4)	1(14)	58
3	Виступ з повідомленням на занятті (Самостійна робота)	2	5	10
4	Залік	4(6)	2(1)	14
Загальна кількість балів				100

Засоби діагностики успішності навчання:

- теоретичні запитання та практичні завдання до лабораторних робіт;
- комплекс тестових завдань для модульного (підсумкового) контролю рівня навчальних досягнень студентів (Див. Рис. 1);
- індивідуальні завдання студентам;
- комплексна контрольна робота.

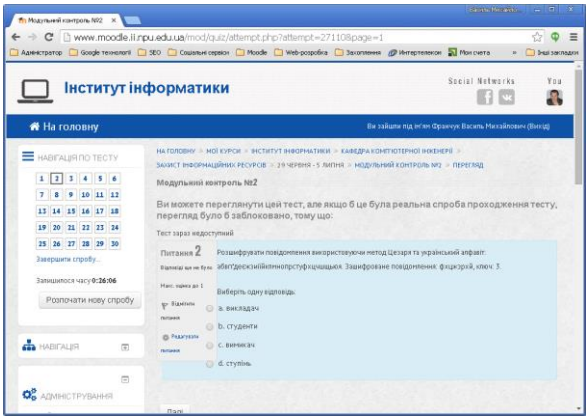

Рис. 1. Приклад тестових завдань для модульного контролю

ДЛЯ ЗАМІТОК