ОПИС

навчальної дисципліни

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ

на 1 семестр 2019-2020 н.р.

Ступінь вищої освіти – магістр
Галузь знань – 01 Освіта/Педагогіка
Напрям підготовки 014.11 Середня освіта (Хімія, Інформатика)

1. Загальна характеристика дисципліни

Загальний обсяг дисципліни – 4 кредити ЄКТС.
Статус дисципліни – вибіркова
Факультет (інститут) – Біолого-природничий факультет
Кафедра – інформатики та інформаційних систем.
Курс – 1; **семестр** – 1; **вид підсумкового контролю** – залік.
Викладачі: канд. техн. наук, доц. Сікора О.В.

Форма навчання	Курс	Семестр	Загальний обсяг дисц.	Кількість годин						Курсова робота	Вид семестрового контролю	
				Аудиторні заняття					Самостійна робота			
			Кредити ЄКТС	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття			Залік	Екзамен
Денна	1	1	4/120	44	16	28			76	-	+	

2. Зміст лекційного матеріалу

Тема 1. Загальні поняття та положення із захисту інформаційних ресурсів.

Поняття інформаційної безпеки. Загрози інформаційній безпеці. Методи і засоби забезпечення інформаційної безпеки. Технології захисту інформаційних ресурсів. Загрози безпеці інформації. Порушники.

Тема 2. ***Основні положення щодо організації системи захисту інформації.***

Умови безпеки інформації. Державна політика і система захисту інформації в Україні. Нормативно-правова база України у сфері захисту інформації. Класифікація шкідливого програмного забезпечення. Захист інформації від вірусів, від несанкціонованого використання та від дефектів. Захист програм від нелегального копіювання й використання. Захист даних на дисках.

Тема 3. Безпека в інформаційних мережах.

Фізична безпека. Загальна характеристика систем захисту в інформаційних мережах. Аутентифікація та безпека мережі. Паролі. Користувацький інтерфейс. Телекомунікації та віддалений доступ. Резервне копіювання. Адміністрування інформаційних систем.

Тема 4. Особливості організації захисту в інформаційно-комунікаційних системах.

Запобігання вторгненням та доступу на рівні підсистеми користувачів, підсистеми управління та каналах зв'язку.

Тема 5. Антивірусні засоби.

Програмні віруси та способи їх нейтралізації. Комп'ютерні віруси та їх властивості. Класифікація вірусів. Основні види комп'ютерних вірусів та схеми їх функціонування. Структура комп'ютерних вірусів. Програми виявлення вірусів та заходи по захисту та профілактиці. Антивірусні пакети.

Тема 6. Криптографічні засоби, шифрування, цифровий підпис.

Основні поняття криптографії та теорії секретних систем. Види шифрування інформації. Перші методи шифрування перестановки та заміни. Одноалфавітні системи шифрування Віженера, Плейфейра та інш. Багато алфавітні системи шифрування: Енігма, Виженера та інш. Їх роль у сучасної криптографії. Симетричні та асиметричні криптографічні системи та їх застосування. Реалізація систем криптографічного захисту інформації. Застосування систем для захисту конфіденційної інформації.

Тема 7. Комплексна система захисту інформації.

Створення комплексної системи захисту інформації. Вимоги до комплексної системи захисту інформації та політика безпеки. Створення і впровадження комплексної системи захисту інформації.

3. Перелік лабораторних робіт та розподіл балів за захист

№	Теми лабораторних робіт	К-ть балів
1	Огляд складових інформаційної безпеки	6
2	Захист інформаційних ресурсів за допомогою пароля	6
3	Дослідження системи захисту інформації на ПК за допомогою BIOS	6
4	Архівація файлів як один із видів захисту інформації	6
5	Програмна реалізація шифру Цезаря, частоколу	6
6	Програмна реалізація шифру Віженера, ширу пар	6
7	Програмна реалізація шифру одноразового блокнота	6
8	Алгоритм шифрування ADFGVX	6
9	Алгоритм шифрування RSA	6
10	Алгоритм шифрування DES	6
11	Підсумкове заняття	
	Разом за __1__семестр:	60

4. Самостійна робота студента

Теми, що виносяться на самостійне опрацювання:

- Основні положення щодо організації системи захисту інформації.
- Визначення інформаційних ресурсів, що підлягають захисту.
- Технології захисту інформаційних ресурсів.
- Захист інформації від вірусів, від несанкціонованого використання та від дефектів.
- Захист інформації в Інтернет-ресурсах.
- Вимоги до комплексної системи захисту інформації та політика безпеки.
- Порівняльний аналіз криптографічних методів захисту інформаційних ресурсів.
- Вимоги до комплексної системи захисту інформації та політика безпеки.

5. Система поточного та підсумкового контролю результатів навчання. Критерії оцінювання.

Формою підсумкового контролю досягнутих успіхів студента з дисципліни є залік.

Досягнуті успіхи студента з дисципліни оцінюються під час виконання та захисту лабораторних робіт та контрольних робіт.

Протягом семестру пропонується виконати 10 *лабораторних робіт*. До захисту необхідно опрацювати поданий у методичних вказівках теоретичний матеріал. За виконання лабораторних завдань можна отримати максимум 60 балів (по 6 балів за кожну лабораторну роботу,). Кількість балів, що виставляється за лабораторне заняття, враховує:

- знання теоретичного матеріалу з теми;
- повноту виконання поставлених завдань з теми;
- своєчасне виконання та захист лабораторної роботи.

Термін захисту лабораторної роботи вважається своєчасним, якщо студент захистив її згідно з графіком. У разі не дотримання термінів захисту лабораторної роботи максимальна кількість балів за роботу зменшується на 1 бал кожні 2 тижня.

Контрольні роботи передбачають виконання тестових та практичних завдань. За виконання контрольної роботи студент може отримати до 40 балів.

Сумарна кількість балів з дисципліни за семестр визначається як поточна успішність (сума балів з усіх видів навчальної роботи). Оцінка виставляється за шкалами оцінювання: стобальною, національною і ЄКТС.

Оцінювання результатів навчання

	Семестр 1
Контрольна робота	40
Захист лабораторних робіт	60
Всього балів	100

Залік за талоном №2 і перед комісією проводиться в письмово-усній формі з оцінюванням за стобальною шкалою.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Белкин П. Ю., Михальський О. О., Першаков А. С. Про- граммно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных. — М.: Радио и связь, 1999. — 168 с.

2. Герасименко В. А. Основы защиты информации.— М.: Ин- комбук, 1997. — 537 с.

3. Домарев В. В. Безопасность информационных технологий. Методы создания систем защиты. — К.: ООО ТИД ДС, 2001. — 688 с. PDF created with FinePrint pdfFactory Pro trial version http://www.fineprint.com 1 3

4. ДСТУ 3396.2–97. Захист інформації. Технічний захист інфор- мації. Терміни і визначення. — К.: Держстандарт України, 1998.

5. Закон України “Про державну таємницю”.

6. Закон України “Про захист інформації в автоматизованих системах”.

7. Закон України “Про інформацію”.

8. Закон України “Про науково-технічну інформацію”.

9. Медведовский И. Д., Семьянов П. В., Леонов Д. Г. Атака на “Internet”. — 2-е изд., перераб. и доп. — М.: ДМК, 1999. — 336 с.

10. НД ТЗІ 1.1–003–99 Термінологія у галузі захисту інфор- мації в комп’ютерних системах від несанкціонованого досту- пу. — К.: Держстандарт України, 1999.

11. НД ТЗІ 2.5–004–99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. — К.: Держстандарт України, 1999.

12. НД ТЗІ 2.5–005–99 Класифікація автоматизованих систем і стандартні профілі захищеності оброблюваної інформації від несанкціонованого доступу. — К.: Держстандарт України, 1999.

13. Петров А. А. Компьютерная безопасность. Криптографичес- кие методы защиты. — М.: ДМК, 2000. — 448 с.

14. ТаненбаумЭ. Современные операционные системы. — СПб.: Питер, 2004. — 848 с.

10. ІНФОРМАЦІЙНІ РЕСУРСИ

1. http://www.dstszi.gov.ua — сайт департаменту спеціальних те- лекомунікаційних систем та захисту інформації СБ України.

Викладач _____ _____
Підпис Ініціали та прізвище

Завідувач кафедрою _____ _____
Підпис Ініціали та прізвище