МІНІСТЕРСТВО КУЛЬТУРИ УКРАЇНИ

ХАРКІВСЬКА ДЕРЖАВНА АКАДЕМІЯ КУЛЬТУРИ

Кафедра інформаційно-документних систем

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в інформаційних системах

(шифр і назва навчальної дисципліни)

РІВЕНЬ ВИЩОЇ ОСВІТИ Перший (бакалаврський)

ГАЛУЗЬ ЗНАНЬ 18 Виробництво та технології

СПЕЦІАЛЬНІСТЬ 186 Видавництво та поліграфія

КВАЛІФІКАЦІЯ бакалавр видавництва та поліграфії

Спеціалізація Технології електронних мультимедійних видань та редагування

Харків — 2017

Робоча програма Захист інформації в інформаційних системах

Розроблено та внесено : Харківська державна академія культури

Розробник: С.О. Мар'їн, канд. техн. наук, доцент, доцент кафедри інформаційно-документних систем

Робоча програма затверджена на засіданні кафедри інформаційно-документних систем

Протокол від «06» листопада 2017 року № 5

Завідувач кафедри інформаційно-документних систем

_____ (Л.Я. Філіпова)
(підпис) (прізвище та ініціали)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="2">Кількість кредитів – 3</td><td>Шифр та назва галузі 18 Виробництво та технології</td><td colspan="2" rowspan="2">Фундаментальна</td></tr>
<tr><td></td></tr>
<tr><td>Модулів – 3</td><td rowspan="4">Шифр та назва спеціальності: 186 Видавництво та поліграфія</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 3</td><td>4-й</td><td>4-й</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання _____ (назва)</td><td colspan="2">Семестр</td></tr>
<tr><td>Загальна кількість годин – 108</td><td>7-й</td><td>8-й</td></tr>
<tr><td rowspan="11">Тижневих годин для денної форми навчання: аудиторних – 2 самостійної роботи студента – 6</td><td rowspan="11">Освітньо-кваліфікаційний рівень: бакалавр</td><td colspan="2">Лекції</td></tr>
<tr><td>12 год.</td><td>10 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>20 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>76 год.</td><td>76 год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання:</td></tr>
<tr><td colspan="2">Вид контролю: іспит</td></tr>
</table>

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

для денної форми навчання – 32/76

для заочної форми навчання – 16/76

2. Мета та завдання навчальної дисципліни

Мета – навчання студентів підходам до захисту комп’ютерної інформації та деякім математичним засобам захисту інформації.

Завдання:

- надати студентам уявлення про сучасні, мережеві погрози комп'ютерної інформації;
- висвітлити базові підходи та принципи створення безпеки комп'ютерної інформації;
- надати студентам уявлення про існуючі програмні засоби захисту комп'ютерної інформації;
- надати студентам уявлення про існуючі закони про захист інформації як в Україні так і

закордоном;
- познайомити з базовими підходами до захисту інформації в кріптології;
- розглянути перелік найбільш розповсюджених алгоритмів захисту інформації;
- розглянути перелік програмних засобів призначених для захисту інформації;
- провести ознайомлення з базовими функціями декількох програмних продуктів захисту інформації.

У результаті вивчення навчальної дисципліни студент повинен

Знати:
- перелік законів України яки так чи інакше пов'язани з захистом інформації взагалі та беспосерньо з захистом комп'ютерної інформації;
- особливості та перелік деструктивних дій різних типів вірусів (обов'язково включаючи до цих типів мережеві віруси);
- стандартну класифікацію та перелік загальних груп закладок-вірусів;
- стислий перелік існуючих програмних засобів до захисту комп'ютерної інформації;
- особливості використання математичних моделей у захисті комп'ютерної інформації;
- базові функції найбільш розповсюдженого антивірусного програмного забезпечення ..

Вміти:
- запускати на виконання антивірусне програмне забезпечення встановлене на комп'ютері;
- здійснювати вибір антивірусного програмного забезпечення;
- здійснювати пошук антивірусного програмного забезпечення в мережі Інтернет та завантаження його на власний комп'ютер;
- використовувати базові функції найбільш поширених антивірусних програмних продуктів (наприклад: Avast, Dr.Web Cureit!, Zillja, Kaspersky AVP Tool та інші).

3. Зміст і структура навчальної дисципліни

.

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		Л	п	С.	інд	с.р.		л	п	с.	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Розділ 1. Загрози комп'ютерної безпеки та підходи до її захисту												
Тема 1. Загрози комп'ютерний безпеки.	13	1		2		10	13	1	2			10
Тема 2. Програми-шпигуни.	13	1		2		10	13	1	2			10
Тема 3. Парольний	14	2		2		10	11	1				10

захист операційних систем.												
Тема 4. Програмний захист комп'ютерної інформації.	14	2		2		10	13	1	2			10
Разом	54	6		8		40	50	4	6			40
Розділ 2. Кріптографія та коп'ютерная безпека												
Тема 5. Введення до крипто-графічних засобів захисту комп'ютерної інформації.	16	2		4		10	11	1				10
Тема 6. Аріфметічна та алгебраична база кріптології.	15	1		4		10	11	1				10
Разом	31	3		8		20	22	2				20
Розділ 3. Інформаційно-комунікаційні інститути суспільства												
Тема 7. Загальні поняття політики информаційної безпеки.	14	2		2		10	3	2				10
Тема 8. Концепція інформаційної безпеки України.	9	1		2		6	10	2				6
Разом	23	3		4		16	20	4				16
Усього годин	108	12		20		76	92	10	6			76

Розділ 1.

Тема 1. Погрози комп'ютерний безпеки.

Комп'ютерна злочинність у країнах СНД, стислий аналіз тенденцій у цій галузі. Всесвітня мережа Internet, як середовище і знаряддя здійснення комп'ютерних злочинів. Методи злому комп'ютерних систем: атаки на рівні операційної системи, атаки на рівні мережевого програмного забезпечення, атаки на рівні систем управління базами даних. Перелік підходів до захисту програмних систем від злому.

Тема 2. Програми-шпигуни.

Програмні закладки: моделі впливу програмних закладок на комп'ютери – перехоплення, перекручення, спостереження та компрометація. Захист від

програмних закладок: захист від впровадження програмних закладок, виявлення впровадженої закладки, видалення програмної закладки. Троянські програми: джерело появи троянських програм, засоби визначення наявності троянської програми на комп'ютері, програми для виявлення троянських програм. Клавіатурні шпигуни: імітатори, фільтри, заступники. Засоби захисту системи від програмних шпигунів.

Тема 3. Парольний захист операційних систем.

Парольні зломщики. Визначення та засоби роботи парольних зломщиків. Злом парольного захисту операційної системи Windows NT: база даних облікових записів користувачів, збереження паролів користувачів, використання паролів, можливі атаки на базу даних.

Тема 4. Програмний захист комп'ютерної інформації.

Перелік підходів до захисту комп'ютерної інформації: програмні засоби, апаратні засоби, організаційні мери. Перелік найбільш розповсюджених програмних засобів: Comodo Antivirus**,** Avira AntiVir Personal**,** Comodo Internet Security**,** avast! Free Antivirus**,** Ad-Aware Free Internet Security**,** Dr.Web CureIt!**,** AVG Anti-Virus Free**,** Kaspersky AVP Tool **,** AVZ Antiviral Toolkit**,** Emsisoft Anti-Malware**,** BitDefender Free Edition**,** Zillya!**,** Panda Cloud Antivirus**,** PC Tools ThreatFire**,** Microsoft Security Essentials**,** PC Tools AntiVirus Free**.** Порівняльні характеристики вказаних вище програмних засобів.

Розділ 2.

Тема 5. Введення до криптографічних засобів захисту комп'ютерної інформації.

Базові терміни криптології: захист інформації, криптографія, криптологія, криптоаналіз, простір повідомлень, простір ключів, простір зашифрованих повідомлень, алфавіт, слово, текст. Етапи розвитку криптографії: перший етап (з найдавніших часів по 1949 р.), другий (з 1949 – 1976 р.), третій (1976 – теперішній час). Стислий перелік дисциплін, яки використовуються в криптології. Коло цікавих фактів з історії розвитку криптології. Перши спроби захисту інформації: шифр Цезаря, гомофоніческое шифрування, полігамне шифрування, біграмне шифрування, шифр Віжінера, шифр Плейфнера.

Тема 6. Аріфметічна та алгебраична база кріптології.

Алгоритм ділення із остачею, найбільший загальний дільник, взаємно-прості числа, найменше загальне кратне, прості числа, порівняння, класи відрахувань, порівняння першого ступеня, система порівнянь першого ступеня, існування першообразного коріння. Поняття групи, підгрупи груп, циклічні групи, гомоморфізми груп, групи підстановок, дія групи на безлічі, кільця й поля, підкільца, гомоморфізми кілець, Евклидови кільця, прості й максимальні ідеали, кінцеві розширення полів, поле розкладання, кінцеві поля, порядки неперекладних багаточленів, лінійні рекурентні послідовності, послідовності максимального періоду.

Розділ 3.

Тема 7. Загальні поняття політики информаційної безпеки.

Визначення та основні поняття політики безпеки. Предмет політики. Принципи політики безпеки. Види моделей політики інформаційної безпеки.

Дискреційна політика безпеки: визначення дискреційної політики безпеки, матриця доступу, приклади варіантів задання матриці доступу, переваги дискреційної політики безпеки, перелік суттевих недоліків дискреційної політики безпеки. Мандатна політика безпеки: визначення мандатної політики безпеки, мандатне управління доступом, пристрій мандатного контролю, монітор звернень, переваги мандатної політики безпеки, недолікі мандатної політики безпеки. Рольова політика безпеки: визначення рольової політики безпеки, перелік ролей, особлівості розподілення повноважень між ролями, особливості формулювання критеріїв безпеки, повний перелік вад та переваг ролевої політики. Значення політики безпеки інформації. Опис трьохрівневої політики інформаційної безпеки. Особливості організації секретного діловодства.

Тема 8. Концепція інформаційної безпеки України.

Державна інформаційна політика України. Комплекс політичних, правових, економічних, соціально -культурних і організаційних заходів української держави в сфері відтворення та розповсюдження інформації. Головними напрямами державної інформаційної політики є: забезпечення доступу кожного до інформації, забезпечення рівних можливостей усіх суб'єктів інформаційних відносин, створення умов для формування в Україні інформаційного суспільства, забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень, створення інформаційних систем і мереж інформації, постійне оновлення, збагачення і зберігання національних інформаційних ресурсів, забезпечення інформаційної безпеки України, формування позитивного іміджу держави; сприяння міжнародній співпраці в інформаційній сфері і вхід України в світовий інформаційний простір. Стисле знайомство з указом президента України № 377/2008 Про рішення Ради національної безпеки і оборони України від 21 березня 2008 року «Про невідкладні заходи щодо забезпечення інформаційної безпеки України».

5. Теми семінарських занять

№ з/п	Назва теми	Кількість Годин
1	Методи злому комп’ютерних систем. Пошук інформації про конкретних людей в мережи.	2
2	Що таке програмні закладки, стилий аналіз.	2
3	Особливости захисту від програмних закладок.	2
4	Визначення та засоби роботи парольних зломщиків	2
5	Троянські програми	2
6	Пошук інформації про антивірусні програмні продукти	4
7	Визначення та основні поняття політики безпеки.	4
9	Державна інформаційна політика України.	2
	Разом	20

6. Теми практичних занять

№	Назва теми	Кількість

з/п		Годин
1	Пошук інформації про конкрену людину у мережі Інтернет.	2
2	Пошук інформації про антивірусні програмні засоби в мережі Інтернет	4
	Разом	6

7. Самостійна робота

№ з/п	Назва теми	Кількість Годин
1.	Методи злому комп'ютерних систем.	10
2.	Різновиди програм-шпіонів	10
3.	Особливості парольного захисту операційних систем	10
4.	Особливості функціонування антівірусних програм	10
5.	Особливості функціонування шифру Плейфнера	10
6.	Робота з діленням з остачею	10
7.	Види моделей політики інформаційної безпеки	10
8.	Ознайомлення з головними напрямами інформаційної політики України	6
	Разом	76

8. Методи навчання

Лекції, семінарські та практичні заняття, самостійна робота, складання схем та порівняльних таблиць.

9. Методи контролю

Поточне тестування, оцінка за реферат, оцінки за відповіді на семінарських заняттях, підсумковий письмовий тест.

10. Розподіл балів, які отримують студенти

Приклад для екзамену

<table>
<tr><td colspan="7">Поточне тестування та самостійна робота</td><td>Підсумковий тест (екзамен)</td><td>Сума</td></tr>
<tr><td colspan="3">Змістовий модуль 1</td><td colspan="2">Змістовий модуль 2</td><td colspan="2">Змістовий модуль 3</td><td rowspan="3">20</td><td rowspan="3">100</td></tr>
<tr><td>Т1</td><td>Т2</td><td>Т3</td><td>Т4</td><td>Т5</td><td>Т7</td><td>Т8</td></tr>
<tr><td>10</td><td>10</td><td>10</td><td>10</td><td>10</td><td>10</td><td>10</td></tr>
</table>

Шкала оцінювання: національна та ECTS

Сума балів за всі	Оцінка	Оцінка за національною шкалою

види навчальної діяльності	ECTS	для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	**A**	відмінно	зараховано
82-89	**B**	добре	
74-81	**C**		
64-73	**D**	задовільно	
60-63	**E**		
35-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

11. Методичне забезпечення

Опорні конспекти лекцій, комплекс навчально-методичного забезпечення дисципліни (КНМЗД); нормативні документи, ілюстративні матеріали.

12. Рекомендована література

Базова

1. Анин Б. Защита компьютерной информации / Б.Анин, — Спб.: БХВ-Петербург, 2000. — 384 с.
2. Спесивцев А. В. Защита информации в персональных ЭВМ / А. В. Спесивцев, В. А. Вегнер, А. Ю. Крутяков и др. — М.Радио и связь, МП «Весту», 1993. — 192 с.
3. Коутинхо С., Введение в теорию чисел. Алгоритм RSA / С. Коутинхо. — М.: Постмаркет. — 2001. — 328 с.
4. Ю.С. Харин Математические основі криптологии: / Учебное пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев. — Мн.: БГУ, 1999. — 319 с.
5. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1996 — 200 с.
6. Biham E. New Types of Criptoanalitic Attack Using Related Keys // J. of Cryptology/ 1991. V4
7. Бернет С., Криптография. Официальное руководство RSA Security / С. Бернет, С. Пэйн. — М.: Бином Год, 2002, — 240 с.
8. Запечников С. В., Криптографические протоколы и их применение в финансовой и коммерческой деятельности / С. В. Запечников. — М.: Горячая Линия - Телеком Год, 2007, — 120 с.
9. Иванов М. А., Криптография. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. — М.: КУДИЦ-Образ Год, 2001 — 24 с.
10. Щербаков А., Прикладная криптография. Использование и синтез криптографических интерфейсов / А. Щербаков, А. Домашев. — М.: Русская Редакция Год, 2003 — 180 с.

11. Аграновский А. В., Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. — М.: Солон-Пресс Год, 2009 — 90 с.
12. Нечаев В. И., Элементы криптографии. Основы теории защиты информации / В. И. Нечаев. — М.: Высшая школа Год, 1999 — 80 с.
13. Баричев С.Г. Основы современной криптографии / С.Г. Баричев, Р.Е. Серов. — М.: Горячая Линия. — 2002. — 153 с.
14. Белов Е.Б, Основы информационной безопасности / Е.Б Белов, В.П. Лось др. — М.: Горячая линя. —Телеком, 2006. — 544 с.
15. Menezes A.J., Handbook of Applied Cryptography / A.J. Menezes, C. Oorschot, S.A. . — Vanstone. : CRC Press. — 1996. — 816 с.

Допоміжна

16. Шнейер Б. Слабые места криптографических систем / Б. Шнейер // Открытые системы. — 1999. — №1.
17. Экни Р. Введение в криптографические стандарты / Р. Экни // Защита информации. «Конфидент». — 1996. — №4.
18. Пробелков П. Сколько стоит «сломать» Netscape? / П. Пробелков // Защита информации. «Конфидент». — 1996. — №5.
19. Левитан Ю.Л., Соболь И.М. О датчике псевдослучайных чисел для персональных компьютеров // Математическое моделирование .— 1990. Т.2., №8, с. 119-126.
20. Мао В., Современная криптография. Теория и практика / В. Мао.— М. : Вильямс Год, 2005 .— 90 с.
21. Панасенко С., Алгоритмы шифрования. Специальный справочник / С. Панасенко.— СПб.: БХВ-Петербург Год .— 2009 .— 250 с.
22. Тилборг Х.К., Основы криптологии. Профессиональное руководство и интерактивный учебник / Х. К. Тилборг.— М.: Мир.— 2006 .— 471 с.
23. Ростовцев А.Г., Теоретическая криптография / А.Г. Ростовцев, Е.Б. Маховенко — М.: Профессионал .— 2005 .— 490 с.
24. Мухачев В.А., Методы практической криптографии / В.А. Мухачев, В.А. Хорошко . — М.: Полиграф-Консалтинг. — 2005. — 209 с.
25. Бабаш А.В., Криптография / А.В. Бабаш, Г.П. Шанкин. — М.: СОЛОН-ПРЕСС. — 2007. — 512 с. - (Серия книг «Аспекты защиты»)
26. В.В. Ященко, Введение в криптографию / В.В. Ященко, Н.П. Варновский, Ю.В. Нестеренко, 3-е изд., доп. — МЦНМО: «ЧеРо» . — 2000. — 288 с.
27. ГОСТ Р 53109 – 2008, Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности.