МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

Програмне забезпечення систем захисту інформації

(назва навчальної дисципліни)

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
до самостійної роботи
з навчальної дисципліни
підготовки докторів філософії

зі спеціальності 122 Комп'ютерні науки та інформаційні технології

2016 рік

РОЗРОБЛЕНО ТА ВНЕСЕНО:
кафедрою інформаційних систем, протокол №11 від 05.04.2016 р.

1. ЗАГАЛЬНІ ВІДОМОСТІ

Самостійна робота здобувача (СРЗ) – це форма організації навчального процесу, за якої заплановані завдання виконуються здобувачем самостійно під методичним керівництвом викладача.

Метою самостійної роботи здобувача в межах навчальної дисципліни "Програмне забезпечення систем захисту інформації" є засвоєння в повному обсязі навчальної програми та формування у здобувачів загальних і професійних компетентностей, які відіграють суттєву роль у становленні майбутнього доктора філософії.

Навчальний час, відведений для самостійної роботи здобувачів очної форми навчання, визначається навчальним планом і становить 74 % (112 години) від загального обсягу навчального часу на вивчення дисципліни (150 годин).

У ході самостійної роботи здобувач має перетворитися на активного учасника навчального процесу, навчитися свідомо ставитися до оволодіння теоретичними і практичними знаннями, вільно орієнтуватися в інформаційному просторі, нести індивідуальну відповідальність за якість власної освітньо-наукової діяльності.

СРЗ в межах навчальної дисципліни "Програмне забезпечення систем захисту інформації" включає:

опрацювання лекційного матеріалу;

опрацювання та вивчення рекомендованої літератури, основних термінів та понять за темами дисципліни;

підготовку до лабораторних занять;

поглиблене опрацювання окремих лекційних тем або питань;

пошук (підбір) та огляд літературних джерел за заданою проблематикою дисципліни;

контрольну перевірку здобувачами особистих знань за запитаннями для самодіагностики;

підготовку до контрольних робіт та інших форм поточного контролю;

систематизацію вивченого матеріалу з метою підготовки до семестрових екзаменів.

2. ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ

Завдання самостійної роботи, які передбачені навчальним планом і програмою навчальної дисципліни для засвоєння теоретичних знань і практичних навичок, наведені в табл. 1.

Таблиця 1

Завдання для самостійної роботи здобувачів та форми її контролю

№ з/п	Компетентності, які забезпечуються	Назва теми	Завдання для самостійної роботи	Кіль-кість годин	Форми контролю СРЗ	Література
	Змістовий модуль І. Правове забезпечення інформаційної безпеки					
1.	здатність формувати політику безпеки на основі використання КСЗІ	Тема 1. Законодавча база щодо формування політики безпеки на основі стандарту ISO/IEC 27001:2013	підготовкаа до лабораторних занять; поглиблене опрацювання окремих лекційних тем або питань; пошук (підбір) та огляд літературних джерел за заданою проблематикою дисципліни контрольна перевірку здобувачами особистих знань за запитаннями для самодіагностики	30	експрес-опитування	Основна: [1 – 3]. Додаткова: [9 – 14]
2.		Тема 2. Класифікація кіберзагроз на основі KDD 99		10	експрес-опитування	Основна: [1 – 5]. Додаткова: [12 – 15]
3.		Тема 3. Побудова системи управління інформаційної безпеки на основі стандарту ISO/IEC 27002:2005		20	контрольна робота	Основна: [1 – 8]. Додаткова: [12 – 15]
Разом за змістовим модулем І				60		
Змістовий модуль ІІ. Програмно-апаратні засоби і методи забезпечення інформаційної безпеки						
4.	здатність формувати політику безпеки на основі використання КСЗІ	Тема 4. Сучасний стан засобів подолання систем захисту. Захист від несанкціонованого копіювання	підготовкаа до лабораторних занять; поглиблене опрацювання окремих лекційних тем або питань; пошук (підбір) та огляд літературних джерел за заданою проблематикою дисципліни контрольна перевірку здобувачами особистих знань за запитаннями для самодіагностики	20	експрес-опитування	Основна: [1 – 5]. Додаткова: [12 – 15]
5.		Тема 5. Моделювання процесів нападу на інформацію та її зв’язок з практичними завданнями		32	контрольна робота	Основна: [1– 6]. Додаткова: [10]
Разом за змістовим модулем ІІ				52		
Разом з навчальної дисципліни				**112**		

3. СИСТЕМА ОЦІНЮВАННЯ УСПІШНОСТІ САМОСТІЙНОЇ РОБОТИ

Виконання кожного завдання для самостійної роботи оцінюється відповідно до

Тимчасового положення “Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою” ХНЕУ ім. С. Кузнеця (табл. 2).

Таблиця 2

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		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	не зараховано
1 – 34	F		

Розподіл балів за виконання завдань для самостійної роботи у межах тем змістових модулів навчальної дисципліни наведено в табл. 3.

Таблиця 3

Розподіл балів за завданнями та змістовними модулями

Завдання для самостійної роботи	Змістовий модуль 1			Змістовий модуль 2		Сума балів
	ЗСР1	ЗСР2	ЗСР3	ЗСР4	ЗСР5	25
Максимальна кількість балів	5	5	5	5	5	

ЗСР– завдання для самостійної роботи здобувача.

Оцінки за цією шкалою заносяться до відомостей обліку успішності та іншої академічної документації.

4. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

4.1. Основна

1. ISO/IEC 27002:2013 Информационные технологии – Методы обеспечения безопасности – Системы менеджмента информационной безопасности — Свод практик для элементов управления информационной безопасностью

2. ISO/IEC 27003, Информационные технологии – Методы обеспечения безопасности – Руководство по внедрению системы менеджмента информационной безопасности

3. ISO/IEC 27004, Информационные технологии – Методы обеспечения безопасности – Менеджмент информационной безопасности – Измерения

4. KDD'99 Competition Dataset, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, (1999).

5. ISO 31000:2009, Менеджмент рисков – Принципы и руководство

6. ISO/IEC 27005, Информационные технологии – Методы обеспечения безопасности – Менеджмент рисков информационной безопасности.

7. Євсеєв С.П. Технології захисту інформації: електр. навч. посібник/ С.П. Євсеєв, С.Е. Остапов, О.Г. Король, Г.П. Коц // ХНЕУ ім. С. Кузнеця, ХНЕУ ім. С. Кузнеця, 2016. – 585 с.

8. Дудатьєв А.В. Захист програмного забезпечення./ А.В. Дудатьєв, В.А. Каплун, В.П. Семеренко// Частина 1. Навчальний посібник. – Вінниця: ВНТУ, 2005. – 140 с.

4.2. Додаткова

9. Євсеєв С.П. Гешування даних в інформаційних системах: монографія/ С.П. Євсеєв, О.Ю. Йохов, О.Г. Король// ХНЕУ, 2013. – 312 с.

10. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень: Монографія / Житомир : Рута, 2010. – 280 с.

11. Бурячок, В. Політика інформаційної безпеки [Текст]: підручник / В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко; під заг. ред. проф. В. О. Хорошка. — К.: ПВП «Задруга», 2014. – 222 с.

12. СОУ Н НБУ 65.1 СУІБ 2.0:2010. Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD)

4.3. Ресурси Інтернет

13. http://www.mathmodels.net/ru/sravnenie-zashchishchennosti-informatsii-v-otkrytoj-i-zakrytoj-setyakh

14. http://www.itsec.ru/articles2/allpubliks

15. http://www.securitylab.ru/

16. https://habrahabr.ru/