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

Програмне забезпечення систем захисту інформації

(назва навчальної дисципліни)

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
до проведення поточного контролю 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

Поточний контроль успішності навчання здобувачів з дисципліни “Програмне забезпечення систем захисту інформації” та рівня сформованості у них компетентностей, які підтримуються даною навчальною дисципліною, здійснюється у таких формах:

- активна участь у навчальній діяльності на лекції, ведення конспекту;
- експрес-опитування;
- захист лабораторних робіт;
- теоретичні контрольні роботи, тестування за матеріалами змістовних модулів.

Поточний контроль успішності навчання здійснюється у формі експрес-опитування на кожному лекційному/лабораторному занятті).

Типовий приклад експрес-опитування наведено у розділі “Завдання для поточного контролю успішності навчання”.

Зазначені форми і засоби поточного контролю успішності навчання здобувачів з навчальної дисципліни “Програмне забезпечення систем захисту інформації” спрямовані на стимулювання систематичної поточної навчальної та самостійної роботи тих, хто навчається, підвищення об’єктивності оцінювання їх знань, запровадження здорової конкуренції між здобувачами у навчанні, виявлення і розвитку їх творчих і дослідницьких здібностей.

Мінімально можлива кількість балів за поточний контроль упродовж семестру – 60.

Результати всіх форм поточного контролю є невід’ємними складовими **критеріїв підсумкового оцінювання знань здобувачів,** наведених у відповідному розділі навчально-методичного забезпечення дисципліни “Програмне забезпечення систем захисту інформації”.

2. ЗАВДАННЯ ДЛЯ ПОТОЧНОГО КОНТРОЛЮ УСПІШНОСТІ НАВЧАННЯ

2.1. Типові приклади завдань для поточного контролю за формами.

2.1.1 Типовий приклад завдань для експрес-опитування за темою лекційного заняття Законодавча база щодо формування політики безпеки на основі стандарту ISO/IEC 27001:2013:

1. Сутність системи управління інформаційною безпекою.
2. Основні етапи розроблення та управління СУІБ.
3. Сутність внутрішніх аудитів СУІБ.

3. СИСТЕМА ОЦІНЮВАННЯ УСПІШНОСТІ НАВЧАННЯ ПІД ЧАС ПРОВЕДЕННЯ ПОТОЧНОГО КОНТРОЛЮ

Система оцінювання успішності навчання здобувача та рівня сформованості у

нього компетентностей, які підтримуються навчальною дисципліною “Програмне забезпечення систем захисту інформації” (Програма навчальної дисципліни “Програмне забезпечення систем захисту інформації”) враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні заняття, а також виконання самостійної роботи).

При розрахунку підсумкової оцінки успішності здобувача з навчальної дисципліни “Програмне забезпечення систем захисту інформації” слід вважати, що кожна форма поточного контролю має різну питому вагу у формуванні його компетентностей, які забезпечуються навчальною дисципліною.

З урахуванням вагомості кожної форми поточного контролю успішність навчання здобувача з навчальної дисципліни у підсумку оцінюється у відповідних балах (табл. 3.1) за формулою:

$$R = A + B + C + D,$$

де R – підсумковий максимальний бал, який здобувач може отримати за успішне виконання усіх форм поточного контролю;

A – максимальна кількість балів, яку здобувач може отримати за активну участь у навчальній діяльності на лекції, ведення конспекту (A = 16);

B – максимальна кількість балів, яку здобувач може отримати за експрес-опитування (B = 24);

C – максимальна кількість балів, яку здобувач може отримати за захист лабораторних завдань (C=20);

Виконання кожного завдання для поточного контролю успішності здобувача оцінюється відповідно до Тимчасового положення “Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою” ХНЕУ ім. С. Кузнеця (табл. 1).

Таблиця 1

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 поточного контролю за формами у межах тем змістових модулів наведено в табл. 2.

Таблиця 2

Розподіл балів за формами поточного контролю та змістовними модулями

Форма поточного контролю	Змістовий модуль 1				Змістовий модуль 2			Сума балів
	активна участь у навчальній діяльності на лекції, ведення конспекту	експрес-опитування	захист лабораторних робіт	теоретичні контрольні роботи	активна участь у навчальній діяльності на лекції, ведення конспекту	експрес-опитування	захист лабораторних робіт	
Максимальна кількість балів	10	12	10	4	6	8	10	60

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

Здобувач отримує право на виконання завдань підсумкового контролю (допуск до залік, якщо кількість балів, одержаних за результатами перевірки успішності під час поточного контролю відповідно до змістового модуля впродовж семестру, в сумі досягла 60 балів.

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/