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

Програмне забезпечення систем захисту інформації
(назва навчальної дисципліни)

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
до лабораторних занять
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

Метою проведення лабораторних занять з 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.

У ході лабораторних занять здобувач набуває професійних компетентностей та практичних навичок роботи з відповідними програмними продуктами.

Відповідно до програми навчальної дисципліни “Програмне забезпечення систем захисту інформації” на лабораторні заняття відводиться 22 год. навчального часу.

Лабораторні заняття з навчальної дисципліни “Програмне забезпечення систем захисту інформації” проводяться у спеціально оснащених обчислювальних центрах Харківського національного економічного університету імені Семена Кузнеця.

За результатами виконання завдання на лабораторному занятті здобувачі формують теку з електронними результатами виконання та захищають їх перед викладачем.

2. ЗАВДАННЯ ДЛЯ ЛАБОРАТОРНИХ ЗАНАНЯТЬ

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

Таблиця 1

Перелік тем та завдань для лабораторних занять

№ з/п	Назва теми	Компетентності, які забезпечуються	Програмні питання і завдання для лабораторних занять	Кіль-кість годин	Форма контро-лю	Необхідне ПЗ*	Література
Змістовий модуль І. Правове забезпечення інформаційної безпеки							
1.	Тема 1. Законодавча база щодо формування політики безпеки на основі стандарту ISO/IEC 27001:2013	здатність формувати політику безпеки на основі використання КСЗІ	ЛР1. Підсистема реєстрації	4	експрес-опитування	ПЗ “Технології захисту інформації”, ОС Linux	Основна: [1 – 3]. Додаткова: [9 – 14]
2.	Тема 2. Класифікація кіберзагроз на основі KDD 99		ЛР2. Дослідження стійкості парольного захисту	4	експрес-опитування		Основна: [1 – 5]. Додаткова: [12 – 15]
3	Тема 3. Побудова системи управління		ЛР3. SQL-ін’єкції та	4			Основна: [1 – 8].

№ з/п	Назва теми	Компетентності, які забезпечуються	Програмні питання і завдання для лабораторних занять	Кіль-кість годин	Форма контро-лю	Необхідне ПЗ*	Література
	інформаційної безпеки на основі стандарту ISO/IEC 27002:2005		методи боротьби з ними				Додаткова: [12 – 15]
Разом за змістовим модулем І – 12							
Змістовий модуль ІІ. Програмно-апаратні засоби і методи забезпечення інформаційної безпеки							
4	Тема 4. Сучасний стан засобів подолання систем захисту. Захист від несанкціонованого копіювання	здатність формувати політику безпеки на основі використання КСЗІ	ЛР3. SQL-ін'єкції та методи боротьби з ними	5	експрес-опитування	ПЗ "Технології захисту інформації", ОС Linux	Основна: [1 – 5]. Додаткова: [12 – 15]
5	Тема 5. Моделювання процесів нападу на інформацію та її зв'язок з практичними завданнями		ЛР4. Дослідження стійкості точок доступу бездротової мережі Wi-Fi	5	експрес-опитування		Основна: [1– 6]. Додаткова: [10]
Разом за змістовим модулем ІІ – 10							
Разом за навчальною дисципліною – 22							

*ПЗ – програмне забезпечення

3. ТИПОВИЙ ПРИКЛАД ЗАВДАННЯ ДЛЯ ЛАБОРАТОРНИХ ЗАНЯТЬ

Лабораторне заняття № 1:
Підсистема реєстрації.

Завдання: визначити основні принципи системи захисту інформації в підсистемах реєстрації.

Мета заняття: ознайомити здобувачів з місцем та задачами підсистеми реєстрації в системах захисту інформації від несанкціонованого доступу

Основні теоретичні відомості: **Підсистема реєстрації** є сукупністю таких механізмів захисту, що здійснюють реєстрацію всіх подій в обчислювальній системі, які прямо чи опосередковано стосуються її безпеки. Використання механізмів реєстрації обумовлено такими чинниками:

1) оскільки обчислювальні системи складаються з великої кількості компонентів та мають дуже складну структуру, практично неможливо гарантувати відсутність помилок при їх розробці, а також адміністративних помилок під час їх експлуатації;

2) побудовані за допомогою криптографічних механізмів захисту системи є вразливими внаслідок можливості розкриття засобами криптоаналізу, а системи, що використовують паролі, – внаслідок можливості підбору паролю;
3) використання систем розмежування доступу обмежує користувачів системи певними правилами, дотримання яких не завжди можна забезпечити організаційними заходами;
4) навіть найдосконаліша система розмежування доступу є вразливою від дій користувачів, що зловживають своїми повноваженнями.

В якості прикладів подій, що реєструються, можна навести включення та виключення системи, вхід у систему та вихід з неї користувачів, невдалі спроби автентифікації, доступ суб'єктів до об'єктів, зміну повноважень суб'єктів по відношенню до об'єктів та інші. Реєстрація має відбуватися як на рівні системного (операційна система), так і на рівні прикладного (наприклад сервер бази даних) програмного забезпечення.

Для реєстрації подій створюється спеціальний файл (або група файлів), що носить назву **журналу реєстрації**. Журнал реєстрації, як правило, містить інформацію про час, дату, місце, тип та результати кожної зареєстрованої події. Система захисту інформації від несанкціонованого доступу повинна забезпечити захист своїх журналів реєстрації від несанкціонованого доступу, знищення або спотворення.

Хід роботи.

1. Доповніть програму, розроблену в ході Лабораторних робіт № 7,8 механізмом реєстрації подій. Обов'язково повинні реєструватися вдалі та невдалі спроби автентифікації та вдалі і невдалі спроби доступу до об'єктів.
2. Відлагодьте програму та запротоколюйте її роботу у вигляді таблиці з двох стовпчиків. Перший має містити дії користувача, другий – їх відображення в журналі аудиту.
3. Оформіть звіт.

Очікуваний результат виконання завдання:

1) вихідні тексти серверної частини програми.
2) протоколи роботи програми.
3) блок-схему; діаграму класів або модулів, або data-flow diagram (на вибір) та діаграму прецедентів розробленого ПЗ (виконуються за допомогою UML – ПЗ);
4) висновок.

4. СИСТЕМА ОЦІНЮВАННЯ УСПІШНОСТІ НАВЧАННЯ

Виконання кожного завдання для лабораторних занять 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 до лабораторних занять у межах тем змістових модулів наведено в табл. 3.

Таблиця 3

Розподіл балів за завданнями та змістовними модулями

Завдання для лабораторних занять	Змістовий модуль 1			Змістовий модуль 2		Сума балів
	ЗЛЗ1	ЗЛЗ2	ЗЛЗ3	ЗЛЗ3	ЗЛЗ4	
Максимальна кількість балів	5	5		5	5	20

ЗЛЗ – лабораторне завдання.

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

5. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

5.1. 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.

5.2. 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)

5.3. 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/