

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

Програмне забезпечення систем захисту інформації

(назва навчальної дисципліни)

ПРОГРАМА
навчальної дисципліни
підготовки докторів філософії

зі спеціальності 122 Комп'ютерні науки та інформаційні технології

2016 рік

РОЗРОБЛЕНО ТА ВНЕСЕНО: Харківський національний економічний університет імені Семена Кузнеця, кафедра інформаційних систем

(повне найменування вищого навчального закладу, кафедри)

РОЗРОБНИКИ ПРОГРАМИ: Євсєєв Сергій Петрович

Обговорено та рекомендовано до затвердження Вченою радою
“25” квітня 2016 року, протокол № 9

ВСТУП

Програма вивчення навчальної дисципліни “Програмне забезпечення систем захисту інформації” складена відповідно до освітньо-наукової програми підготовки докторів філософії зі спеціальності “122 Комп’ютерні науки та інформаційні технології”.

Предметом вивчення навчальної дисципліни є вивчення основних вимог щодо формування політики безпеки на основі використання програмного забезпечення комплексних систем захисту інформації.

Міждисциплінарні зв’язки: “Вища математика”, “Операційні системи”, “Технології захисту інформації”, “Мережеві технології”.

Програма навчальної дисципліни складається з таких змістових модулів:

1. Правове забезпечення інформаційної безпеки.
2. Програмно-апаратні засоби і методи забезпечення інформаційної безпеки.

1. Мета та завдання навчальної дисципліни

1.1. Метою викладання навчальної дисципліни “Програмне забезпечення систем захисту інформації” є навчання студентів принципам побудови комплексних систем захисту інформації, дослідженню та використанню сучасних процедур забезпечення основних услуг безпеки інформації, що засновані на використанні алгоритмів симетричної та несиметричної криптографії в комунікаційних системах, протоколів інфраструктури відкритих ключів (ІВК).

1.2. Основними завданнями вивчення дисципліни “Програмне забезпечення систем захисту інформації” є аналіз законодавчої бази щодо формування політики безпеки на основі стандарту ISO/IEC 27001:2013, дослідження основних кіберзагроз на основі класифікації KDD 99, основні вимоги стандарту ISO/IEC 27002:2005 щодо побудови системи управління інформаційної безпеки (СУІБ), дослідження основних методів оцінки кібернападу, методик оцінки економічних втрат, побудови моделей моделювання процесів нападу на інформацію та її захисту, методів двофакторній автентифікації, та портативних засобів захисту інформації.

1.3. Згідно з вимогами освітньо-наукової програми здобувачі освітньо-наукового ступеня “доктор філософії” набувають таку компетентність – здатність формувати політику безпеки на основі використання КСЗІ.

На вивчення навчальної дисципліни відводиться 150 годин, 5 кредитів ЄКТС.

2. Інформаційний обсяг навчальної дисципліни

Змістовий модуль 1. Правове забезпечення інформаційної безпеки

Тема 1. Законодавча база щодо формування політики безпеки на основі стандарту ISO/IEC 27001:2013

Тема 2. Класифікація кіберзагроз на основі KDD 99

Тема 3. Побудова системи управління інформаційної безпеки на основі стандарту ISO/IEC 27002:2005

Змістовий модуль 2. Програмно-апаратні засоби і методи забезпечення інформаційної безпеки

Тема 4. Сучасний стан засобів подолання систем захисту. Захист від несанкціонованого копіювання

Тема 5. Моделювання процесів нападу на інформацію та її зв'язок з практичними завданнями

3. Рекомендована література

1. Ленков С. В. Методы и средства защиты информации : монография [в 2-х т.] Т. 2. Информационная безопасность / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – К. : Арий, 2008. – 344 с.

2. Євсєєв С.П. Захист інформації в інформаційних системах. Методи традиційної криптографії: навч. посібник/ С.П. Євсєєв, О.О. Кузнецов, О.Г. Король// ХНЕУ, 2010. – 314 с.

3. Євсєєв С.П. Захист інформації в інформаційних системах. навч. посібник/ С.П. Євсєєв, О.О. Кузнецов, О.Г. Король// ХНЕУ, 2011. – 510 с.

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

5. Остапов С.Е. Технології захисту інформації: навч. посібник/ С.Е. Остапов, С.П. Євсєєв, О.Г. Король// Чернівці : Родовід, 2014. – 427 с.

6. Остапов С.Е. Технології захисту інформації: навч. посібник/ С.Е. Остапов, С.П. Євсєєв, О.Г. Король// ХНЕУ ім. С. Кузнеця, 2013. – 475 с.

7. Євсєєв С.П. Технології захисту інформації: електр. навч. посібник/ С.П. Євсєєв, 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.

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

- 4. Форма підсумкового контролю успішності навчання – залік**
- 5. Засоби діагностики успішності навчання – експрес-опитування, контрольна робота.**