Міністерство освіти і науки України
І ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
ЕНІ МИХАЙЛА КОЦЮБИНСЬКОГО
тут магістратури, аспірантури і докторантури
Кафедра інноваційних та інформаційних технологій в освіті

ЗАТВЕРДЖУЮ
Ректор Вінницького
державного педагогічного
університету імені Михайла
Коцюбинського
_____доц. Лазаренко Н.І.
29 вересня 2016 р.

ПП.15 ТЕОРІЯ ЗАХИСТУ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

ПРОГРАМА

нормативної навчальної дисципліни

підготовки бакалавра
галузі знань 0101 Педагогічна освіта
напряму підготовки 6.010104 Професійна освіта. Комп'ютерні технології в управлінні та навчанні

РОЗГЛЯНУТО І СХВАЛЕНО
на засіданні навчально-методичної комісії навчально-наукового інституту педагогіки, психології, підготовки фахівців вищої кваліфікації
Протокол №1 від 27 вересня 2016р

РОЗГЛЯНУТО І СХВАЛЕНО
на засіданні Вченої ради Вінницького державного педагогічного університету імені Михайла Коцюбинського
Протокол №4 від 28.09. 2016р

Вінниця - 2016 рік

УДК 004.056.5(073)
ББК 32.973.26-8.2р30
К 43

Розробники:
Кізім Світлана Степанівна, кандидат педагогічних наук, доцент кафедри інноваційних та інформаційних технологій в освіті інституту магістратури, аспірантури, докторантури.
Люльчак Світлана Юріївна, кандидат педагогічних наук, старший викладач кафедри інноваційних та інформаційних технологій в освіті інституту магістратури, аспірантури, докторантури.
Рецензенти:
Гуревич Роман Семенович – доктор педагогічних наук професор, член-кореспондент НАПН України, директор Інституту магістратури, аспірантури, докторантури;
Петрук Віра Андріївна – доктор педагогічних наук професор Вінницького національного технічного університету

К 43 Кізім С.С. Теорія захисту даних в інформаційних системах [Текст]: програма нормативної навчальної дисципліни / С. С. Кізім, С. Ю. Люльчак. - Вінниця : ВДПУ імені Михайла Коцюбинського, 2016. – 9 с.

Програма навчальної дисципліни «Теорія захисту даних в інформаційних системах» складена відповідно до основних положень організації навчального процесу у ВНЗ, вимог державних стандартів освіти України, освітньо-професійної програми підготовки фахівців галузі знань 0101 Педагогічна освіта напряму підготовки 6.010104 Професійна освіта. Комп`ютерні технології в управлінні та навчанні. В програмі розкрито принципи побудови систем захисту інформації та застосування механізмів захисту інформації.

Програма затверджена на засіданні кафедри інноваційних та інформаційних технологій в освіті протокол № 1 від 29 серпня 2016 року
Завідувач кафедри інноваційних та інформаційних технологій в освіті
_____ проф. Кадемія М.Ю.

Програма розглянута і схвалена на засіданні навчально-методичної комісії навчально-наукового інституту педагогіки, психології, підготовки фахівців вищої кваліфікації
Протокол № 1 від 27 вересня 2016 року

Голова _____ Коломієць Л.І.

ВСТУП

Навчальна дисципліна "Теорія захисту даних в інформаційних системах" відноситься до дисциплін підготовки студентів з спеціальності і дає теоретичні та практичні основи організації та забезпечення технічного та криптографічного захисту даних в інформаційних системах.

Програма вивчення нормативної навчальної дисципліни «Теорія захисту даних в інформаційних системах» складена відповідно до освітньо-професійної програми підготовки спеціалістів галузі знань «0101 Педагогічна освіта» напряму підготовки «6.010104 Професійна освіта. Комп`ютерні технології в управлінні та навчанні».

Предметом вивчення навчальної дисципліни є принципи побудови систем захисту інформації, застосування механізмів захисту інформації, що засновані на використанні алгоритмів традиційної (симетричної) криптографії, криптографії з відкритим ключем, MAC-кодів і геш- функцій для забезпечення автентичності, цілісності та конфіденційності інформації в інформаційних системах (ІС). Розглянуто основи стеганографічного захисту інформації та особливості побудови інфраструктури відкритих ключів (ІВК).

Міжпредметні зв'язки. Вивчення дисципліни «Теорія захисту даних в інформаційних системах» базується на дисциплінах «Принципи побудови та захист інформації баз даних», «Практикум з виробничого навчання», «Застосування комп`ютерних технологій в управлінні», «Прикладне програмування». Вивчення дисципліни "Теорія захисту даних в інформаційних системах" дозволяє студентам оволодіти знаннями та вміннями, які створять теоретичний і практичний фундамент, необхідний для аналізу загроз виникаючих при зберіганні, обробленні та передачі інформації; побудові системи захисту інформації на основі використання методів традиційної криптографії та криптографії з відкритим ключем. Матеріал цієї дисципліни використовується у подальшому вивченні дисциплін професійно-педагогічної підготовки, під час виконання студентами домашніх завдань, лабораторних, практичних та курсових робіт із дисциплін, пов'язаних із використанням інформаційно-комунікаційних технологій (ІКТ) і професійним становленням

висококваліфікованого фахівця у галузі «Професійна освіта. Комп'ютерні технології в управлінні та навчанні».

Програма навчальної дисципліни складається з таких змістових модулів:

Змістовий модуль 1. Основи технічного захисту даних в інформаційних системах.

Змістовий модуль 2. Методи та системи криптографічного захисту даних в інформаційних системах.

1.1. *Метою* вивчення навчальної дисципліни «Теорія захисту даних в інформаційних системах» є формування у студентів системи знань в галузі інформаційної безпеки інформаційних систем.

1.2. *Основними завданнями* вивчення дисципліни «Теорія захисту даних в інформаційних системах» є:

- одержання фундаментальних знань в галузі технічного і криптографічного захисту даних;
- оволодіння навичками виявлення загроз даних в інформаційних системах і забезпечення їхньої інформаційної безпеки;
- виховання у студентів методичних навичок в творчому застосуванні знань по професійному призначенню.

1.3. Згідно з вимогами освітньо-професійної програми студенти повинні:

знати:

- вимоги нормативно-керівних документів України з технічного захисту інформації в системах зв'язку та інформатизації;
- основні методи та заходи захисту інформаційно-телекомунікаційних систем від витоку інформації технічними каналами;
- основи забезпечення технічного та криптографічного захисту інформації;

уміти:

- забезпечувати виконання вимог відповідальних нормативно-керівних

документів України по захисту інформації в телекомунікаційних системах;

- створювати обґрунтування та вибір необхідних заходів по забезпеченню захисту інформації в телекомунікаційних системах;
- проводити необхідний комплекс заходів по забезпеченню безпеки зв`язку та інформації на телекомунікаційних об'єктах;
- бути ознайомленими з сучасним станом та тенденціями розвитку засобів та систем захисту інформації в інформаційно-телекомунікаційних системах.

На вивчення навчальної дисципліни відводиться 54 годин / 1,5 кредити ECTS/.

2. Інформаційний обсяг навчальної дисципліни

Змістовий модуль 1. Основи технічного захисту даних в інформаційних системах

Тема 1. Основи технічного захисту інформації в телекомунікаційних системах

Сучасний стан безпеки інформації та методи забезпечення недоступності даних. Технічні канали витоку інформації. Сучасний зв'язок, його уразливість, поняття каналу витоку інформації, забезпечення недоступності даних. Класифікація, характеристика та порівняння акустичних, акусто-перетворювальних, електромагнітних та оптичних каналів витоку інформації.

Загрози безпеки для інформаційно-телекомунікаційних систем та теоретичні основи протидії витоку інформації технічними каналами витоку.

Поняття загроз, їх класифікація та аналіз, пристроїв скритого зняття інформації. Узагальнена математична модель каналу витоку інформації, теоретично та практично неінформативні канали, основні методи досягнення неінформативності технічного каналу витоку інформації.

Тема 2. Методи захисту інформації в телекомунікаційних системах

Практична протидія витоку інформації по технічним каналам. Методи

та пристрої протидії знищенню інформації.

Загальні рекомендації, пасивна та активна протидія, екранування, захист ліній зв'язку. Пасивна та активна протидія знищенню інформації, захист телефонних апаратів.

Пошук пристроїв несанкціонованого доступу.

Аналізатори телефонних ліній, індикатори поля, скануючі приймачі.

Змістовний модуль 2. Методи та системи криптографічного захисту даних в інформаційних системах.

Тема 3. Методи криптографічного захисту інформації в інформаційно-телекомунікаційних системах

Основи криптографії, елементи теорії чисел. Теоретичні основи криптографічного захисту інформації. Модулярна арифметика та її застосування в криптографії. Принципи та методи криптографічного захисту, їх класифікація.

Шифрування методами перестановки та простої заміни. Шифрування методами складної заміни, гамування.

Перестановки та прості заміни, рішення прикладів. Складні заміни, гамування, рішення прикладів.

Теоретична та практична стійкість криптографічних систем.

Теорія Шеннона, вимоги до ключів у досконалій секретній системі, розсіювання та перемішування. Короткий історичний огляд криптографії.

Тема 4. Системи криптографічного захисту інформації

Сучасні симетричні системи шифрування – DES вітчизняний стандарт. Історія створення, режими роботи.

Асиметрична система шифрування - RSA. Принцип дії, односпрямовані функції, безпека та швидкість дії.

Асиметричні системи шифрування: схема Поліга-Хеллмана, Схема Ель-Гамаля, комбінований метод шифрування. Принципи роботи схем, порівняння з іншими асиметричними схемами шифрування.

3. Рекомендована література

Основна

1. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький // Львів: Науково-технічна література, 1998. – 248 с.

2. Горбатов В. С. Основы технологии PKI / В. С. Горбатов, О. Ю. Полянская // – М.: Горячая линия – Телеком. 2004. – 248 с.

3. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев // – М.: СОЛОН-Прес, 2002. – 272 с.

4. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. / А. А. Петров //– М.: ДМК, 2000. – 448 с.

5. Пономаренко В. С. Основи захисту інформації. Навчальний посібник / В. С. Пономаренко, І. В Журавльова // – Харків: Вид. ХДЕУ, 2003. – 176 с. Столлингс В. Криптография и защита сетей: принципы и практика Пер. с англ. / В. Столлингс // – 2-е изд. – М.: Издательский дом "Вильямс", 2001. – 672 с.

6. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов // – СПб.: Наука и Техника, 2004. – 384 с.

Додаткова

1. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян. Н. А. Молдовян // – 2-е изд. – СПб.: БХВ-Петербург, 2003. – 368 с.

2. Чмора А. Л. Современная прикладная криптографія / А. Л. Чмора // – М.: Гелиос АРВ. 2001. – 256 с.

3. Баранов О. А. Інформаційне право України: стан. проблеми. перспективи / О. А. Баранов // – К.: Видавничий дім "СофтПрес". 2005. – 316 с.

4. Есин В. И. Безопасность информационньїх систем и технологий / В. И. Есин, А. А. Кузнецов, Л. С. Сорока // - Х. : ООО «ЗДЗНА», 2010. - 656 с.

5. Конахович Г.Ф. Защита информации в телекоммуникационних системах / Г.Ф. Конахович, В.П. Климчук, С.М. Паук // - К. : «МК-Пресс», 2005. - 288 с.

6. Карпова Т.С. Бази даних: моделі, розробка, реалізація / Т.С. Карпова // - СПб : Пітер, 2002. - 304 с.

7. Кузін А.В. Розробка баз даних у системі Microsoft Access: Підручник / А.В. Кузін, В. М. Дьомін // - Форум : Инфра-М., 2005 р.

8. Шаньгин В. Ф. Информационная безопасность компьютерних систем и сетей : учеб. Пособие / В. Ф. Шаньгин // - М. : ИД «ФОРУМ» : ИНФРА-М, 2011 - 416 с.

9. ДСТУ 3396.2-97 Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення.

10. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» затверджений наказом ДСТСЗІ СБ України від 04.12.2000 р. № 53.

11. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп`ютерних системах від несанкціонованого доступу», затверджений наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22.

12. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу», затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22.

13. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22.

14. НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі» затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р.

№ 22.

Internet - ресурси

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» : *за станом на 1 січня 2013 р.* / Верховна Рада України. - Офіц. вид. - Режим доступу до ресурсу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?m'eg=80%2F94-%E2%F0

2. Закон України «Про інформацію» : *за станом на 1 січня 2013 р.* / Верховна Рада України. - Офіц. вид. - Режим доступу до ресурсу: http: //zakon.rada.gov.ua/cgi-bin/laws/main. cgi?nreg=2657-12

3. Портал безпека [Електронний ресурс]. - Режим доступу : URL : www.bezpeka.com - Назва з екрану.

4. Пошукова система у базі лекцій, наукових статей, навчальних посібників та підручників з усього світу / Google Академія - Режим доступу до ресурсу: http://scholar.google.com.ua/

Сайт Державної служби спеціального зв'язку та захисту інформації / — Офіц. вид. - Режим доступу до ресурсу: http://dstszi.kmu.gov.ua

4. Форма підсумкового контролю успішності навчання: залік.

5.Засоби діагностики успішності навчання:

- усне опитування;
- перевірка виконання і захист лабораторних робіт;
- тестування;
- оцінювання виконання самостійної роботи студентів;
- письмова поточна контрольна робота;
- індивідуальна робота над проектом бази даних;
- підсумкова письмова контрольна робота.

Міністерство освіти і науки України

ВІННИЦЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ

імені Михайла Коцюбинського

==========

Р І Ш Е Н Н Я

Вченої ради

Від 28.09 2016р.

Протокол № 4

СЛУХАЛИ: Затвердження авторських програм дисциплін вищої школи.
Інформує секретар Вченої ради доц. Лапшина І.М.

УХВАЛИЛИ: Навчальну програму КІЗІМ С.С., ЛЮЛЬЧАК С.Ю. з дисципліни „Теорія захисту даних в інформаційних системах" для студентів галузі знань 0101 „Педагогічна освіта", напряму підготовки 6.010104 „Професійна освіта. Комп'ютерні технології в управлінні та навчанні" (освітньо-кваліфікаційний рівень – бакалавр) вищих педагогічних закладів освіти з а т в е р д и т и.

Заст. голови Вченої ради (проф. Зінько Ю.А.)

Вчений секретар (доц. Лапшина І.М.)

З г і д н о :

Вчений секретар доц. Лапшина І.М.