Форма № Н-3.03у

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КРЕМЕНЧУЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ МИХАЙЛА ОСТРОГРАДСЬКОГО

Захист інформації в комп'ютерних системах
(назва навчальної дисципліни)

ПРОГРАМА
нормативної навчальної дисципліни

підготовки бакалавра

зі спеціальності 123 «Комп'ютерна інженерія»

освітньо-професійна програма «Комп'ютерна інженерія»

КРЕМЕНЧУК 2020

РОЗРОБЛЕНО ТА ВНЕСЕНО: Кременчуцький національний університет імені Михайла Остроградського

РОЗРОБНИК ПРОГРАМИ: д.т.н., проф. Гученко М.І.

Обговорено та рекомендовано до видання методичною комісією КрНУ за спеціальністю 123 "Комп’ютерна інженерія"

Протокол від “ ___ ” _____ 2020 року № __

Голова _____ (Гученко М. І.)

ВСТУП

Програма вивчення нормативної навчальної дисципліни "Захист інформації в комп’ютерних системах" складена відповідно до освітньо-професійної програми спеціальності 123 – "Комп’ютерна інженерія".

Предметом вивчення навчальної дисципліни є методи та засоби захисту інформації в комп’ютерних системах та мережах, зокрема методи ідентифікації, аутентифікації та авторизації об’єктів і суб’єктів комп’ютерних систем та мереж, засоби захисту програмних продуктів від несанкціонованого використання, засоби криптографії, криптоаналізу та захисту від шкідливих програм.

Міждисциплінарні зв’язки: Дисципліна "Захист інформації в комп’ютерних системах" базується на знаннях та вміннях, отриманих при вивченні дисциплін "Системне програмування", "Теорія інформації та кодування", "Теорія ймовірності та математична статистика", "Системне програмне забезпечення", "Операційні системи", "Архітектура комп’ютера".

Програма навчальної дисципліни складається з таких змістових модулів:

Змістовний модуль 1. Методи та засоби забезпечення інформаційної безпеки в сучасному інформаційно-обчислювальному просторі

Тема 1. Проблеми захисту інформації в обчислювальних системах та мережах.

Тема 2. Ідентифікація, аутентифікація та авторизація суб’єктів та об’єктів комп’ютерних систем та мереж.

Тема 3. Криптографічний захист інформації.

Тема 4. Симетричні та асметричні криптосистеми.

Змістовний модуль 2. Методи та засоби забезпечення інформаційної безпеки та стійкості комп’ютерних технологій та мереж

Тема 5. Основи захисту комп’ютерних мереж.

Тема 6. Комп'ютерні віруси.

Тема 7. Криптографічні протоколи.

Тема 8. Управління криптографічними ключами.

1. Мета та завдання навчальної дисципліни

1.1. Метою викладання навчальної дисципліни "Захист інформації в

комп’ютерних системах" є набуття студентами загальних теоретичних і практичних знань з питань інформаційної безпеки комп’ютерних систем, напрямків загроз, основних принципів організації захисту, структури та функцій системи захисту, та набуття практичних навичок застосування засобів захисту при проектуванні та експлуатації комп’ютерних систем та мереж.

1.2. Основними завданнями вивчення дисципліни "Захист інформації в комп’ютерних системах" є набуття студентами теоретичних знань про основні положення теорії захисту інформації, методи захисту комп’ютерних технологій та мереж, набуття студентами навичок практичного застосування методів криптографії та криптоаналізу, вирішення задач ідентифікації, аутентифікації та авторизації об’єктів та суб’єктів комп’ютерних систем та мереж, навичок захисту програмних продуктів від несанкціонованого використання, а також набуття студентами навичок створення та використання засобів захисту інформації та навичок захисту ПК і комп’ютерних мереж від шкідливих програм.

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

знати :

– основні загрози, принципи і методи захисту;

– основні поняття криптографії та криптоаналізу;

– алгоритми сучасних симетричних та асиметричних криптосистем;

– методи та засоби захисту інформації в комп’ютерних мережах від несанкціонованого доступу;

– методи та засоби захисту ПК та комп’ютерних мереж від шкідливого програмного забезпечення.

вміти :

– підбирати паролі та грамотно користуватись ними;

– шифрувати та дешифрувати повідомлення за допомогою простих криптосистем;

– організовувати захист інформації від шкідливого програмного забезпечення;

– організовувати захист від атак через мережу Internet.

На вивчення навчальної дисципліни відводиться 150 годин / 5 кредитів ECTS.

2. Інформаційний обсяг навчальної дисципліни

Змістовий модуль 1. Методи та засоби забезпечення інформаційної безпеки в сучасному інформаційно-обчислювальному просторі

Тема 1. Проблеми захисту інформації в обчислювальних системах та мережах

Основні властивості інформації, як предмета захисту. Основні проблеми захисту інформації. Види і цілі вторгнень. Напрями загроз. Напрями і засоби захисту інформації. Моделі захисту інформації. Класи захищеності обчислювальних систем та мереж. Основні принципи проектування систем захисту інформації.

Тема 2. Ідентифікація, аутентифікація та авторизація суб'єктів та об'єктів комп'ютерних систем та мереж

Структурно-функціональна схема системи захисту. Основні етапи аутентифікації та авторизації. Фактори аутентифікації. Парольна аутентифікація. Аутентифікація на основі коректної обробки алгоритмів. Аутентифікація на основі електронних та фізичних ключів. Біометрична аутентифікація. Авторизація. Реєстрація подій в системі.

Тема 3. Криптографічний захист інформації

Основні поняття криптографії та криптоаналізу. Криптографічне перетворення. Симетричні та асиметричні криптографічні перетворення. Основні методи криптоаналізу.

Тема 4. Симетричні та асиметричні криптосистеми

Види симетричних шифрів. Абсолютно стійкий шифр. Методи генерації псевдовипадкових числових послідовностей. Блочні та поточні шифри. Принципи побудови сучасних симетричних шифрів. Основні сучасні стандарти симетричного шифрування. Модулярна арифметика. Односторонні функції та їх властивості. Отримання великих простих чисел. Хеш-функції, їх основні властивості. Сучасні асиметричні криптосистеми.

Змістовий модуль 2. Методи та засоби забезпечення інформаційної безпеки та стійкості комп'ютерних технологій та мереж

Тема 5. Основи захисту комп'ютерних мереж

Моделі захисту мереж. Служби захисту. Управління доступом. Протидія міжмережевому несанкціонованому доступу. Міжмережеве екранування. Організація

безпечного віддаленого доступу. Стратегії безпеки. Захищені протоколи.

Тема 6. Комп'ютерні віруси

Класифікація комп'ютерних вірусів. Способи маскування вірусів. Технології проникнення та вбудування (маскування) вірусів. Засоби захисту від вірусів. Методи знешкодження вірусів.

Тема 7. Криптографічні протоколи

Криптографічні протоколи, їх цілі та властивості. Протоли аутентифікації користувачів. Протоколи аутентифікації повідомлень. Електронний цифровий підпис. Відмітка про час створення файлу.

Тема 8. Управління криптографічними ключами

Генерація криптографічних ключів. Зберігання ключів. Розподіл ключів.

3. Рекомендована література

Базова

1. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000. – 384 с.

2. Антонюк А.О. Основи захисту інформації в автоматизованих системах: Навч. посібн. – К.: Видавн. дім. «КМ Академія», 2003. – 244 с.

3. Баричев С. Криптография без секретов. – М.: Горячая линия–Телеком, 2004. – 43 с.

4. Баричев С.Г., Серов Р.Е. Основы современной криптографии. – М.: Горячая Линия–Телеком, 2006. – 152 с.

5. Беляев Д., Гольчевский Ю. Введение в криптографию: Учебн. пособие. – Сыктывкар: Изд-во Сыктывкарского ун-та, 2004. – 152 с.

6. Вертузаєв М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібн. – К.: Вид. Європ. ун-ту, 2001. – 321 с.

7. Гайкович В.Ю. Основы безопасности информационных технологий: Учебн. пособие. – М.: Изд-во МИФИ, 1995. – 93 с.

8. Гундарь К.Ю, Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. – К.: Корнейчук, 2000. – 152 с.

9. Домарев В.В. Безопасность информационных технологий. Системный подход. – К.: ООО "ТИД ДС", 2004. – 992с.

10. Емельянов С.Л., Стрельцов А.А. Основы информационной безопасности. – О.: Юрид. лит, 2003. – 198 с.

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

12. Кузьменко Б.В. Захист інформації. Частина 1. Конспект лекцій: Навчальний посібник К.: Видавничий центр КНУКІМ, 2012. – 172 с.

13. Локхарт Э. Антихакинг в сети. Трюки. – СПб.: Питер, 2005. – 296 с.

14. Лужецький В. А. Основи організаційного захисту інформації: Навч. посібник. – Вінниця: ВНТУ, 2005. – 148 с.

15. Мельников В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – 368 с.

16. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – СПб.: Издательство "Лань", 2001. – 224 с.

17. Петраков А.В. Основы практической защиты информации. – М.: Радио и связь, 2001. – 368 с.

18. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. – М.: Академия, 2006. – 240 с.

19. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е узд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.

20. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.. Защита информации в компьютерных системах и сетях. – М: "Радио и связь", 1999. – 328 с.

21. Саломаа А. Криптография с открытым ключом: Пер. с англ. – М.: Мир, 1995. – 320 с.

22. Семкин С.Н., Беляков Э.В. и др. Основы организационного обеспечения информационной безопасности объектов информатизации. – М.: "Гелиос АРН", 2005. – 158 с.

23. Синадский Н. И., Хорьков Д. А. Защита информации в компьютерных сетях: Учеб. пособие. – Екатеринбург: УрГУ, 2008. – 225 с.

24. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.

25. Скляров Д.В., Искусство защиты и взлома информации. – СПб.: БХВ-Петербург, 2004. – 288 с.

26. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с.

27. Столлингс Вильям. Криптография и защита сетей: принципы и практика. – 2-е изд. / Пер. с англ. – М.: Вильямс, 2001. – 672 с.

28. Терехов А.В., Чернышов В.Н., Селезнев А.В., Рак И.П. Защита компьютерной информации: Учеб. пособие. – Тамбов: Изд-во ТГТУ, 2003. – 80 с.

29. Технология защиты информации в Интернете: Спец. справ. – СПб.: Питер, 2002. – 844 с.

30. Трасковский А.В. Секреты BIOS. – 2-е изд., перераб. и доп. – СПб.: БВХ-Петербург, 2006. – 480 с.

31. Харин Ю.С., Берник В.И., Матвеев Г.В. Математические и компьютерные основы криптологии. – Мн.: Новое знание, 2003. – 382 с.

32. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2002. – 816 с.

Допоміжна

1. Андреєв В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки: Підручник. – К.: Вид. ДУІКТ, 2009. – 292 с.

2. Андрончик А. Н., Богданов В. В., Домуховский Н. А. Защита информации в компьютерных сетях. Практический курс. – Екатеринбург: УГТУ-УПИ, 2008. – 248 с.

3. Бабаш А.В. Информационная безопасность. Лабораторный практикум: учебное пособие для студентов вузов. – М. : КНОРУС, 2012. – 136 с.

4. Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 р. № 851-IV.

5. Закон України "Про захист інформації в автоматизованих системах", Закон України "Про цифровий підпис" від 22 травня 2003 р. № 852-IV.

6. Кан Д. Война кодов и шифров: История 4-х тысячелетий криптографии / Пер. с англ. Е. Алексеева. – М.: РИПОЛ Классик, 2004. – 528 с.

7. Кнут Д. Исскуство программирования. Том 3. Сортировка и поиск, 2-е издание.: Пер. с .англ. – М. : ООО "И.Д. Вильямс", 2007. – 832 с.

8. Малахов Ю.А. Защита интеллектуальной собственности: Учеб. пособие. – Брянск: БГТУ, 2005. – 96 с.

9. Програма інформатизації НАН України Проект "Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ" Шифр – КСЗІ АІС НАНУ Технічні рішення щодо захисту web-серверів 05540149.90000.043.ИЗ-04, 2008.

10. Симонович С.В. Информатика: Базовый курс. – СПб.: Питер, 2002. – 640 с.

11. Устенко І.В. Системи захисту інформації: Навч. посібник. – Миколаїв: НУК, 2006. – 68 с.

12. Форристал Д. Защита от хакеров Web-приложений: учеб. пособие. – М.: ДМК Пресс, 2008. – 496 с.

4. Форма підсумкового контролю успішності навчання іспит.

5. Засоби діагностики успішності навчання 2 контрольні роботи, опитування, практичні роботи за індивідуальними завданнями.