Форма № Н – 3.04у

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КРЕМЕНЧУЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ МИХАЙЛА ОСТРОГРАДСЬКОГО
Кафедра комп’ютерних та інформаційних систем

“ЗАТВЕРДЖУЮ”
Проректор з науково-педагогічної
та методичної роботи

_____В.В. Костін
“_____”_____2020 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в комп’ютерних системах

спеціальність 123 "Комп’ютерна інженерія"

Факультет електроніки і комп’ютерної інженерії

КРЕМЕНЧУК 2020

Робоча програма "Захист інформації в комп’ютерних системах" для студентів спеціальності 123 "Комп’ютерна інженерія". «___» _____ 2020 року – 13 с.

Розробник: М. І. Гученко, д.т.н., професор, професор кафедри комп’ютерних та інформаційних систем

Робоча програма затверджена на засіданні кафедри комп’ютерних та інформаційних систем

Протокол від «___» _____ 2020 року № __

Завідувач кафедри комп’ютерних та інформаційних систем

_____ (Гученко М. І.)

Схвалено методичною комісією КрНУ за спеціальністю 123 "Комп’ютерна інженерія"
Протокол від «____» _____ 2020 року № ___

Голова _____ (Гученко М. І.)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td colspan="2">денна форма навчання</td></tr>
<tr><td>Кількість кредитів*
5</td><td>Галузь знань
0501 «Інформатика та обчислювальна техніка»</td><td colspan="2">Нормативна</td></tr>
<tr><td rowspan="2">Модулів – 1</td><td rowspan="5">Спеціальність:
123 «Комп’ютерна інженерія»</td><td colspan="2">Рік підготовки:
(курс)</td></tr>
<tr><td>4-й</td><td></td></tr>
<tr><td>Змістових модулів – 2</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 150</td><td>8-й</td><td></td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 5
самостійної роботи студента – 10</td><td rowspan="10">Освітньо-кваліфікаційний рівень:
бакалавр</td><td>24 год.</td><td>-</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>26 год.</td><td>-</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>100 год.</td><td>-</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>іспит</td><td>-</td></tr>
</table>

Примітка.
Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить:

для денної форми навчання – 50/150 = 0,3

* 1 кредит = 30 год.
Кількість кредитів =150/30=5.

2. Мета та завдання навчальної дисципліни

Мета: засвоєння студентами базових 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.

Завдання:

– вивчення студентами основних положень теорії захисту інформації;

– набуття студентами загальних теоретичних знань про основні методи захисту комп'ютерних технологій та мереж;

– набуття студентами навичок практичного застосування методів криптографії та криптоаналізу;

– набуття студентами навичок вирішення задач ідентифікації, аутентифікації та авторизації об'єктів та суб'єктів комп'ютерних систем та мереж;

– набуття студентами навичок захисту програмних продуктів від несанкціонованого використання;

– набуття студентами навичок створення та використання засобів захисту інформації;

– набуття студентами навичок захисту ПК та комп'ютерних мереж від шкідливих програм.

У результаті вивчення навчальної дисципліни студент повинен

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.

уміти:

– 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.

3. Програма навчальної дисципліни

Модуль 1

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.

Модуль 2

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.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	денна форма				
	усього	у тому числі			
		л	п	лаб	с.р.
1	2	3	4	5	6
Модуль 1. Методи та засоби забезпечення інформаційної безпеки в сучасному інформаційно-обчислювальному просторі.					
Тема 1. Проблеми захисту інформації в обчислювальних системах та мережах.	16	2	-	2	12
Тема 2. Ідентифікація, аутентифікація та авторизація суб'єктів та об'єктів комп'ютерних систем та мереж.	18	2	-	4	12
Тема 3. Криптографічний захист інформації.	20	4	-	4	12
Тема 4. Симетричні та асметричні криптосистеми.	20	4	-	4	12
Разом за модулем 1	74	12	-	14	48
Модуль 2. Методи та засоби забезпечення інформаційної безпеки та стійкості комп'ютерних технологій та мереж					
Тема 5. Основи захисту комп'ютерних мереж.	20	4	-	4	12
Тема 6. Комп'ютерні віруси.	16	2	-	2	12
Тема 7. Криптографічні протоколи.	20	4	-	4	12
Тема 8. Управління криптографічними ключами.	16	2	-	2	12
Разом за модулем 2	72	12	-	12	48
ІНДЗ (КР)	-	-	-	-	-
Семестровий контроль (іспит)	4	-	-	-	4
Усього годин	150	24		26	100

5. Теми лабораторних занять

№	Тема лабораторної роботи	Кількість годин
Модуль 1		
1	Захист індивідуального ПК.	2
2	Ідентифікація, аутентифікація, авторизація.	4
3	Криптографія та криптоаналіз.	4
4	Асиметричні шифри та їх криптоаналіз.	4
	Усього за модулем 1	14

№	Тема лабораторної роботи	Кількість годин
Модуль 2		
5	Комп'ютерні віруси та антивірусні програми.	4
6	Мережевий захист персонального комп'ютера.	2
7	Електронно-цифровий підпис.	4
8	Інформаційна безпека глобальної мережі.	2
	Усього за модулем 2	12
	Всього	26

6. Самостійна робота

№ з/п	Назва теми	Кількість годин
		дфн
Модуль 1		
1	Моделі захисту інформації. Класи захищеності обчислювальних систем та мереж. Основні принципи проектування систем захисту інформації.	12
2	Аутентифікація на основі електронних та фізичних ключів. Біометрична аутентифікація. Авторизація. Реєстрація подій в системі.	12
3	Основні методи криптоаналізу.	12
4	Методи генерації псевдовипадкових числових послідовностей. Основні сучасні стандарти симетричного шифрування. Отримання великих простих чисел. Хеш-функції, їх основні властивості.	12
	Усього за модулем 1	48
	Модуль 2	
5	Організація безпечного віддаленого доступу. Стратегії безпеки.	12
6	Методи знешкодження вірусів.	12
7	Протоли аутентифікації користувачів. Протоколи аутентифікації повідомлень.	12
8	Розподіл ключів.	12
	Усього за модулем 2	48
	Усього забезпечення аудиторних занять*	96
	Забезпечення індивідуальних завдань (КР)	-
	Забезпечення семестрового контролю	4
	Усього	100

Примітка:

* – кількість годин самостійної роботи, відведених на підготовку до лекцій, практичних занять, лабораторних робіт та ін. види аудиторної роботи

7. Індивідуальні завдання

Не передбачаються.

8. Методи навчання

При викладанні дисципліни використовуються наступні методи навчання: пояснювально-ілюстративні (розповіді та пояснення з використанням ілюстративного матеріалу, презентацій в MS PowerPoint) та проблемного викладу (ситуаційне моделювання, синектичний аналіз, розв'язання кейсів, написання рефератів). Організація навчання здійснюється за кредитно-модульною системою з елементами тестування та рейтинговим оцінюванням знань студентів у відповідності з Концепцією впровадження в Україні Болонського процесу.

9. Методи контролю

В процесі вивчення дисципліни застосовуються наступні види контролю:

– поточний контроль знань студентів впродовж семестру, який впливає на результати атестацій;

– підсумковий контроль знань студентів (іспит).

	Поточне тестування та самостійна робота										
Вид занять	Модуль 1				Модуль2				КР	Іс-пит	Сума
	Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8			
Лекції	2	2	4	4	4	2	4	2			24
Лабораторні роботи	4	5	5	5	5	3	5	4			36
Модульний контроль				5				5			10
Курсова робота											-
Самост. робота									10		10
Іспит										20	20
Всього	6	7	9	14	9	5	9	11	10	20	100

10. Розподіл балів, що отримують студенти

Шкала оцінювання: національна та ECTS

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Оцінка ECTS</td><td colspan="2">Оцінка за національною шкалою</td></tr>
<tr><td>для екзамену, курсового проекту (роботи), практики</td><td>для заліку</td></tr>
<tr><td>90-100</td><td>A</td><td>відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>незадовільно з можливістю повторного складання</td><td>не зараховано з можливістю повторного складання</td></tr>
<tr><td>0-34</td><td>F</td><td>незадовільно з обов’язковим повторним вивченням дисципліни</td><td>не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

11. Методичне забезпечення

1. Тексти лекцій (електронний варіант). Під час лекційного курсу застосовуються слайдові презентації, виконані у програмі Microsoft Power Point, роздатковий матеріал, здійснюється дискусійне обговорення проблемних питань.
2. Тематичний план викладання дисципліни.
3. Методичні вказівки до виконання лабораторних робіт (електронний варіант). На лабораторних роботах детально розглядаються теоретичні матеріали, розв’язуються завдання за індивідуальними варіантами, використовуються IBM-сумісні персональні комп’ютери, операційні системи Windows і Linux.

12. 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.

15. Інформаційні ресурси

1. Беляев А.В. Методы и средства защиты информации. Интернет-издание. 2005. – [Електронний ресурс]. – Режим доступа: www.citforum.ru/security/ belyaev_book.

2. Бібліотека процедур криптографічного захисту інформації "Тайфун-PKI PKCS#11". – [Електронний ресурс]. – Режим доступа: http://www.ict.com.ua/?lng= 1&sec= 7&art-=2&st=1.

3. Введение в программные системы и их разработку. Национальный Открытый Университет "ИНТУИТ" 2016 г. 650 с. – [Електронний ресурс]. – Режим доступа: www.knigafund.ru/tags/252

4. Виды информационных угроз и способы борьбы с ними. – [Електронний ресурс]. – Режим доступа: http://www.dokwork.ru/2012/01/blog-post.html.

5. Галатенко В.А. Основы информационной безопасности: Учеб. Курс. – [Електронний ресурс]. – Режим доступу: http://www.intuit.ru/department/security/ secbasics/.

6. Руководство по многоуровневой антивирусной защите. Microsoft solutions for security. – [Електронний ресурс]. – Режим доступа: http://technet.microsoft.com/ ru-ru/library/cc162791.aspx.

7. Типы атак на сайты. – [Електронний ресурс]. – Режим доступа: http://it-sec.com.ua/info/tipy-atak-na-sayty.

8. Чеканов Д. Настройка BIOS: руководство. – [Електронний ресурс]. – Режим доступу: http://www.thg.ru/mainboard/ 20050926/nastroyka_bios-09.html.