МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
"Курский государственный университет"

Кафедра информационной безопасности

УТВЕРЖДЕНО

протокол заседания
Ученого совета от 24.04.2017 г., №10

Рабочая программа дисциплины
Защита программ и данных

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация: бакалавр

Факультет физики, математики, информатики

Форма обучения: очная

Общая трудоемкость 2 ЗЕТ

Виды контроля в семестрах:

зачет(ы) 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	17			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	16	16	16	16
В том числе инт.	8	8	8	8
Итого ауд.	32	32	32	32
Контактная работа	32	32	32	32
Сам. работа	40	40	40	40
Итого	72	72	72	72

Курск 2017

Рабочая программа дисциплины Защита программ и данных / сост. к.т.н., Крыжевич Л.С.;; Курск. гос. ун-т. - Курск, 2017. - с.

Рабочая программа составлена в соответствии со стандартом, утвержденным приказом Минобрнауки России от 1 декабря 2016 г. № 1515 "Об утверждении ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата)" (Зарегистрировано в Минюсте России 20 декабря 2016 г. № 44821)

Рабочая программа дисциплины "Защита программ и данных" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность профиль Безопасность компьютерных систем

Составитель(и):

к.т.н., Крыжевич Л.С.;

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Целью освоения учебной дисциплины «Защита программ и данных » является формирование у студентов знаний и умений по защите компьютерной информации с применением современных программно-аппаратных средств.
1.2	Задачи дисциплины – дать знания:
1.3	• о методах и средствах защиты информации в компьютерных системах;
1.4	• о защитных механизмах, реализованных в средствах защиты компьютерных систем от несанкционированного доступа (НСД);
1.5	• о современных программно-аппаратных комплексах защиты информации;
1.6	• о применении средств криптографической защиты информации и средств защиты от НСД для решения задач обеспечения информационной безопасности.
1.7	Приобретенные знания и навыки позволят студентам работать в должностях администраторов компьютерных сетей и администраторов безопасности. Содержание дисциплины охватывает круг вопросов, связанных с обеспечением информационной безопасности кибернетических систем. Особое внимание уделяется обеспечению безопасности автоматизированных систем управления технологическими процессами.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.Б

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ОПК-7: Способностью определять информационные ресурсы , подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объектов защиты
Знать:
основы компьютерной обработки данных, принципы структурной организации вычислительных систем и компьютерных сетей;
Основные угрозы и характеристику технических каналов утечки информации
основные руководящие и нормативные документы по инженерно-технической защите информации
Уметь:
выявлять угрозы и технические каналы утечки информации
применять наиболее эффективные методы и средства инженерно-технической защиты информации
моделировать объекты защиты и угрозы безопасности информации
Владеть:
практическими навыками в использовании основных методов и средств технической защиты информации
навыками применения руководящих и нормативных документов по инженерно-технической защите информации
навыками программирования прикладных задач

ПСК-1.1: Способностью участвовать в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах
Знать:
методы разработки формальных моделей политики безопасности
классификацию и общую характеристику управления доступом и информационными потоками в компьютерных системах
основные принципы политики безопасности
Уметь:
применять методы разработки формальных моделей политики безопасности
применять классификацию политики управления доступом информационными потоками в компьютерных системах
применять правила упраления доступ и информационными потоками в компьютерных системах
Владеть:
методами разработки формальных моделей политики безопасности
методами классификации политики управления доступом информационными потоками в компьютерных системах
методами упраления доступом и информационными потоками в компьютерных системах

ПСК-1.2: Способностью использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований
Знать:
особенности реализации математических методов и алгоритмов

методы дискретного логарифмирования
принципы решения задач факторизации больших чисел
Уметь:
применять теорию вычетов для создания програмных средств
выбирать и использовать математические методы для кодирования информации
применять современные методы криптозащиты при исследовании и проектировании защитных систем
Владеть:
навыками разработки математических методов, алгоритмов шифрования и расшифрования
навыками дискретного логарифмитрования для защиты информации в профессиональной деятельности
способом применения современных математических методов криптозащиты при исследовании и проектировании защитных систем

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем	Вид занятий	Семестр / Курс	Часов	Интеракт.
	Раздел 1. Раздел 1. Информационная безопасность и защита информации» как учебная дисциплина. Основные термины и определения	Раздел			
1.1	Введение	Лек	6	2	0
1.2	Понятие информационной безопасности.. Проблема информационной безопасности в кибернетических системах.понятие доверенной информационной системы.	Ср	6	4	0
1.3	Виды угроз информационной безопасности и характеристика информационных атак	Лек	6	2	2
1.4	Виды угроз информационной безопасности и характеристика информационных атак	Пр	6	2	0
1.5	Виды угроз информационной безопасности и характеристика информационных атак	Ср	6	6	0
1.6	Рубежный контроль	Пр	6	2	0
	Раздел 2. Раздел 2. Информационные угрозы и их классификация	Раздел			
2.1	Принципы системности, комплексности, непрерывности защиты, разумной достаточности, гибкости управления, открытости алгоритмов.	Лек	6	2	2
2.2	Принципы системности, комплексности, непрерывности защиты, разумной достаточности, гибкости управления, открытости алгоритмов.	Ср	6	4	0
2.3	Понятия утечки информации. Классификация основных каналов утечки информации. Способы защиты от утечки информации по техническим каналам.	Лек	6	2	2
2.4	Понятия утечки информации. Классификация основных каналов утечки информации. Способы защиты от утечки информации по техническим каналам.	Пр	6	2	0
2.5	Понятия утечки информации. Классификация основных каналов утечки информации. Способы защиты от утечки информации по техническим каналам.	Ср	6	4	0

2.6	Криптографические методы защиты. Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Электронная цифровая подпись.	Лек	6	2	0
2.7	Криптографические методы защиты. Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Электронная цифровая подпись.	Пр	6	2	0
2.8	Криптографические методы защиты. Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Электронная цифровая подпись.	Ср	6	6	0
2.9	Рубежный контроль	Пр	6	2	0
	Раздел 3. Раздел 3 Технологии применяемые для защиты электронных и компьютерных сетей и баз данных	Раздел			
3.1	Технологии аутентификации. Аутентификация, авторизация и администрирование. Методы аутентификации, использующие пароли	Лек	6	2	0
3.2	Технологии аутентификации. Аутентификация, авторизация и администрирование. Методы аутентификации, использующие пароли	Пр	6	2	0
3.3	Технологии аутентификации. Аутентификация, авторизация и администрирование. Методы аутентификации, использующие пароли	Ср	6	4	0
3.4	Технологии межсетевых экранов. Функции межсетевых экранов. Особенности функционирования межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов.	Лек	6	2	2
3.5	Технологии межсетевых экранов. Функции межсетевых экранов. Особенности функционирования межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов.	Пр	6	2	0
3.6	Технологии межсетевых экранов. Функции межсетевых экранов. Особенности функционирования межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов.	Ср	6	4	0
3.7	Сбор информации системами обнаружения атак. Методы обнаружения информационных атак. Противодействие информационным атакам.	Лек	6	2	0

3.8	Сбор информации системами обнаружения атак. Методы обнаружения информационных атак. Противодействие информационным атакам.	Ср	6	6	0
3.9	Рубежный контроль	Пр	6	2	0
3.10	Итоговое занятие	Зачёт	6	2	0

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для проведения текущего контроля по дисциплине "Защита программ и данных" рассмотрены и одобрены на заседании кафедры от «30» марта 2017 г. протоколом № 8, является приложением к рабочей программе.

5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для проведения промежуточной аттестации по дисциплине "Защита программ и данных" рассмотрены и одобрены на заседании кафедры от «30» марта 2017 г. протоколом № 8, является приложением к рабочей программе.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Заглавие	Эл. адрес	Кол-
Л1.1	Нестеров С. А. - Информационная безопасность: Учебник и практикум - М.: Издательство Юрайт, 2017.	http://www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7	1

6.1.2. Дополнительная литература

	Заглавие	Эл. адрес	Кол-
Л2.1	Шаньгин В.Ф. - Информационная безопасность и защита информации: учебное пособие - Саратов: Профобразование, 2017.	http://www.iprbookshop.ru/63594.html	1

6.3.1 Перечень программного обеспечения

7.3.1.1	199:
7.3.1.2	Microsoft Windows 7 (Open License: 47818817)
7.3.1.3	Microsoft Office 2007 (OpenLicense: 43136274)
7.3.1.4	Adobe Acrobat Reader DC (Бес-платное программное обеспечение)
7.3.1.5	GoogleChrome (Свободная лицензия BSD)
7.3.1.6	7-Zip (Свободная лицензия GNU LGPL),
7.3.1.7	Visual Studio Community (Проприе-тарная академическая лицензия)
7.3.1.8	СКЗИ "КриптоПроCSP" версии 4.0
7.3.1.9	СС КонсультантПлюс (Договор № 7/3Ц от 14.02.2017),
7.3.1.10	СКМ-21 ПО (Компакт-диск со специ-альным программным обеспечением)
7.3.1.11	Смарт-ПО (Компакт-диск с про-граммным обеспечением)
7.3.1.12	Code::Blocks (Свободная лицензия GNU GPLv3)
7.3.1.13	EclipseNeon (Открытое программное обеспечение EclipsePublicLicense)
7.3.1.14	
7.3.1.15	146:
7.3.1.16	Microsoft Windows 7 (OpenLi-cense: 47818817)
7.3.1.17	Ms OfficeProfessional 2007 (OpenLicense: 47818817

7.3.1.18	Google Chrome (Свободная ли-цензия BSD)
7.3.1.19	7-Zip (Свободная лицензия GNU LGPL)
7.3.1.20	Adobe Acrobat Reader DC (Бес-платное программное обеспе-чение)
6.3.2 Перечень информационных справочных систем	
7.3.2.1	Каталог библиотеки КГУ. - Режим доступа: http://195.93.165.10:2280
7.3.2.2	Электронная библиотека.- Режим доступа: http://elibrary.ru
7.3.2.3	Университетская информационная система «Россия» – http://uisrussia.msu.ru
7.3.2.4	Электронная библиотечная система «КнигаФонд» − http://www.knigafund.ru/
7.3.2.5	Электронная библиотечная система «IPRbooks» − http://www.iprbookshop.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Лаборатория программно-аппаратных средств обеспечения информационной безопас-ности;
7.2	Лаборатория технических средств защиты информации;
7.3	для проведения занятий лекци-онного типа, занятий семинаркого типа, курсового проекти-рования (выполнения курсовых работ), групповых и индивиду-альных консультаций, текуще-го контроля и промежуточной аттестации, самостоятельной работы,
7.4	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 199.
7.5	Моноблок LenovoC560 – 9 шт.
7.6	Стенд информационный 1,4м*0,9м – 9 шт.
7.7	Малогабаритный камуфлирован-ный блокиратор работы сотовых телефонов и закладных устройств – 1 шт.
7.8	Селективный обнаружитель циф-ровых радиоустройств ST062 – 1 шт.
7.9	Устройство защиты объектов ин-форматизации от утечки инфор-мации за счет ПЭМИН «Блокада» – 1 шт.
7.10	Нелинейный локатор «Буклет-2» – 1 шт.
7.11	Устройство МП—1А – 1 шт.
7.12	Электронно-оптическое устройст-во для обнаружения любых типов оптических устройств «Гранат» – 1 шт.
7.13	Программно-аппаратный ком-плекс «Соболь» – 1 шт.
7.14	ИМФ-3 имитатор многофункцио-нальный – 1 шт.
7.15	МониторЖК-панель 17 Acep – 1 шт.
7.16	Жалюзи вертикальные тканевые – 1 шт.
7.17	Концентратор 24порт – 1 шт.
7.18	Лабораторный комплекс «Беспро-водные сети ЭВМ»
7.19	Система активной защиты рече-вой акустической информации SEL-157 "Шагрень",
7.20	Устройство «Смарт (Комплекс оценки эффективности защиты речевой информации от утечки по акустическому, виброакустиче-скому и акустоэлектрическому каналам),
7.21	Программно-аппаратные средства защиты информации от НСД .
7.22	
7.23	Помещение для самостоятельной работы обучающихся – аудитория, оснащенная компьютерной техни-кой с возможностью подключения к сети "Интернет" и с обеспечением доступа в электронную информационно-образовательную среду университета.
7.24	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 146.
7.25	Столов – 61
7.26	Посадочных мест – 162
7.27	Компьютеров:
7.28	Для пользователей – 40
7.29	Для библиотекаря – 2
7.30	Моноблоков MSI (27) - модель MS-A912, 2гб оперативной памяти, Athlon CPU D525 1.80GHz
7.31	Моноблоков Asus (13) - модель ET2220I, 4гб оперативной памяти, Intel Core i3-3220 CPU 3.30 GHz
7.32	
7.33	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Студентам необходимо ознакомиться с содержанием рабочей программы, с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками, имеющимся на кафедре.
1.1. Указания по подготовке к занятиям лекционного типа

Изучение дисциплины требует систематического и последовательного накопления знаний, поэтому студентам рекомендуется перед очередной лекцией просмотреть по конспекту материал предыдущей. При затруднениях в восприятии материала следует обращаться к основным литературным источникам, к лектору (по графику его консультаций) или к преподавателю на занятиях семинарского типа.

1.2. Указания по подготовке к лабораторным занятиям
Лабораторные занятия имеют следующую структуру:
- тема занятия;
- цели проведения занятия по соответствующим темам;
- задания состоят из выполнения практических заданий, примеров;
- рекомендуемая литература.

«Методические указания по подготовке к практическим занятиям по дисциплине «Защита программ и данных» утверждены на заседании кафедры от «30» марта 2017 г. протоколом № 8, находятся на кафедре «Программного обеспечения и администрирования информационных систем» в свободном доступе для студентов.

1.3. Методические указания по выполнению самостоятельной работы

Самостоятельная работа студентов включает в себя выполнение практических заданий, самостоятельное изучение отдельных вопросов по теме. По каждой теме учебной дисциплины студентам предлагается перечень заданий для самостоятельной работы, которые содержатся в «Методических указаниях по самостоятельной работе по дисциплине «Защита программ и данных»», утвержденных на заседании кафедры от «30» марта 2017 г. протоколом № 8 и находятся на кафедре « Программного обеспечения и администрирования информационных систем» в свободном доступе для студентов.

1.4. Методические указания по работе с литературой

Основная литература к данной дисциплине - это учебники и учебные пособия.
Дополнительная литература - это монографии, сборники научных трудов, журнальные и газетные статьи, различные справочники, энциклопедии, интернет ресурсы.

В учебнике/ учебном пособии/ монографии следует ознакомиться с оглавлением и научно-справочным аппаратом, прочитать аннотацию и предисловие. Целесообразно ее пролистать, рассмотреть иллюстрации, таблицы, диаграммы, приложения. Такое поверхностное ознакомление позволит узнать, какие главы следует читать внимательно, а какие прочитать быстро.
Студенту следует использовать следующие виды записей при работе с литературой:
Конспект - краткая схематическая запись основного содержания научной работы. Целью является не переписывание произведения, а выявление его логики, системы доказательств, основных выводов.
Цитата - точное воспроизведение текста. Заключается в кавычки. Точно указывается страница источника.
Тезисы - концентрированное изложение основных положений прочитанного материала.
Аннотация - очень краткое изложение содержания прочитанной работы.
Резюме - наиболее общие выводы и положения работы, ее концептуальные итоги и другие виды.