МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное образовательное учреждение высшего образования
"Курский государственный университет"

Кафедра информационной безопасности

УТВЕРЖДЕНО

протокол заседания
Ученого совета от 29.04.2019 г., №9

Рабочая программа дисциплины
Безопасность автоматизированных систем

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Профиль подготовки: Автоматизированные системы обработки информации

Квалификация: бакалавр

Форма обучения: очная

Общая трудоемкость 3 ЗЕТ

Виды контроля в семестрах:

зачет(ы) 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	9,7			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Лабораторные	36	36	36	36
В том числе инт.	2	2	2	2
Итого ауд.	54	54	54	54
Контактная работа	54	54	54	54
Сам. работа	54	54	54	54
Итого	108	108	108	108

Курск 2019

Рабочая программа дисциплины Безопасность автоматизированных систем / сост. к.т.н., Крыжевич Л.С.;; Курск. гос. ун-т. - Курск, 2019. - с.

Рабочая программа составлена в соответствии со стандартом, утвержденным приказом Минобрнауки России от 19.09.2017 г. № 929 "Об утверждении ФГОС ВО по направлению подготовки 09.03.01 Информатика и вычислительная техника (уровень бакалавриата)"

Рабочая программа дисциплины "Безопасность автоматизированных систем" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 09.03.01 Информатика и вычислительная техника профиль Автоматизированные системы обработки информации

Составитель(и):

к.т.н., Крыжевич Л.С.;

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Целью освоения учебной дисциплины «Безопасность автоматизированных систем » 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.В.ДВ.02

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-5: Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения
Знать:
основы работы системного администратора
методы осуществления процесса управления безопасностью ПО
средства осуществления процесса управления безопасностью сетевых устройств
Уметь:
управлять административным процессом управления
осуществлять поддержку административного процесса управления необходимым ПО
быстро и эффективно решать сложившиеся критические ситуации в работе системного администратора
Владеть:
базовым опытом для решения профессиональных задач
знаниями, необходимыми для осуществления безопасного процесса управления администрированием сетевых устройств
навыками, необходимыми для работы системного администратора

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	8	2	0
1.2	Понятие информационной безопасности.. Проблема информационной безопасности в кибернетических системах.понятие доверенной информационной системы.	Ср	8	10	0
1.3	Понятие информационной безопасности.. Проблема информационной безопасности в кибернетических системах.понятие доверенной информационной системы.	Лаб	8	4	0
1.4	Виды угроз информационной безопасности и характеристика информационных атак	Лек	8	2	0

1.5	Виды угроз информационной безопасности и характеристика информационных атак	Лаб	8	4	0
1.6	Виды угроз информационной безопасности и характеристика информационных атак	Ср	8	6	0
1.7	Рубежный контроль	Лаб	8	4	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	8	2	0
2.2	Принципы системности, комплексности, непрерывности защиты, разумной достаточности, гибкости управления, открытости алгоритмов.	Лаб	8	4	0
2.3	Принципы системности, комплексности, непрерывности защиты, разумной достаточности, гибкости управления, открытости алгоритмов.	Ср	8	8	0
2.4	Понятия утечки информации. Классификация основных каналов утечки информации. Способы защиты от утечки информации по техническим каналам.	Лек	8	2	0
2.5	Понятия утечки информации. Классификация основных каналов утечки информации. Способы защиты от утечки информации по техническим каналам.	Лаб	8	4	0
2.6	Понятия утечки информации. Классификация основных каналов утечки информации. Способы защиты от утечки информации по техническим каналам.	Ср	8	8	0
2.7	Криптографические методы защиты. Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Электронная цифровая подпись.	Лек	8	2	0
2.8	Криптографические методы защиты. Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Электронная цифровая подпись.	Лаб	8	4	0
2.9	Криптографические методы защиты. Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Электронная цифровая подпись.	Лек	8	2	0

2.10	Криптографические методы защиты. Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Электронная цифровая подпись.	Ср	8	6	0
2.11	Рубежный контроль	Лаб	8	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	8	2	0
3.2	Технологии аутентификации. Аутентификация, авторизация и администрирование. Методы аутентификации, использующие пароли	Лаб	8	2	0
3.3	Технологии аутентификации. Аутентификация, авторизация и администрирование. Методы аутентификации, использующие пароли	Ср	8	4	0
3.4	Технологии межсетевых экранов. Функции межсетевых экранов. Особенности функционирования межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов.	Лек	8	2	2
3.5	Технологии межсетевых экранов. Функции межсетевых экранов. Особенности функционирования межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов.	Лаб	8	4	0
3.6	Технологии межсетевых экранов. Функции межсетевых экранов. Особенности функционирования межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов.	Ср	8	4	0
3.7	Сбор информации системами обнаружения атак. Методы обнаружения информационных атак. Противодействие информационным атакам.	Лек	8	2	0
3.8	Сбор информации системами обнаружения атак. Методы обнаружения информационных атак. Противодействие информационным атакам.	Ср	8	6	0
3.9	Рубежный контроль	Лаб	8	4	0
3.10	Итоговое занятие	Зачёт	8	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 23.04.2019 г., протокол №11

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 23.04.2019 г., протокол №11

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/ЗЦ 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 утверждены на заседании кафедры от «23» апреля 2019 г. протоколом № 11, находятся на кафедре «Информационной безопасности» 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, утвержденных на заседании кафедры от «23» апреля 2019 г. протоколом № 11 и находятся на кафедре «Информационной безопасности» 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.