

Документ подписан простой электронной подписью
Информация о владельце:

ФИО: Худин Александр Николаевич

Должность: Ректор

Дата подписания: 26.01.2021 12:23:15

Уникальный программный ключ:

08303ad8de1c60b987361de7085acb509ac3da145741b561afbbe37e3a19

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

Информационная безопасность автоматизированных систем

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация: бакалавр

Факультет физики, математики, информатики

Форма обучения: очная

Общая трудоемкость 3 ЗЕТ

Виды контроля в семестрах:

зачет(ы) 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	7 (4.1)		Итого	
	Неделя			
Вид занятий	уп	рп	уп	рп
Лекции	36	36	36	36
Лабораторные	18	18	18	18
В том числе инт.	20	20	20	20
Итого ауд.	54	54	54	54
Контактная работа	54	54	54	54
Сам. работа	54	54	54	54
Итого	108	108	108	108

Рабочая программа дисциплины Информационная безопасность автоматизированных систем / сост. ; 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 "Информационная безопасность автоматизированных систем" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность профиль Безопасность компьютерных систем

Составитель(и):

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	формирование у студентов знаний, умений и навыков, необходимых для построения и анализа безопасных компьютерных систем и технологий.
-----	--

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:	Б1.В.ОД
--------------------	---------

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)**ОК-1: Способностью использовать основы философских знаний для формирования мировоззренческой позиции****Знать:**

сущность и задачи комплексной системы защиты информации

Уметь:

классифицировать информацию по степеням конфиденциальности

Владеть:

технологией организационного управления

ОК-5: Способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики**Знать:**

методологические основы комплексной системы защиты информации

Уметь:

оценивать угрозы безопасности информации

Владеть:

методикой выявления каналов несанкционированного доступа к информации

ОПК-6: Способностью применять приёмы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности**Знать:**

источники, способы и результаты дестабилизирующего воздействия на информацию в случае возникновения чрезвычайных ситуаций

Уметь:

определять причины, обстоятельства и условия дестабилизирующего воздействия на информацию

Владеть:

методами оценки защищенности предприятия

ПК-4: Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
Знать:
источники, способы и результаты дестабилизирующего воздействия на информацию
Уметь:
определять возможные методы несанкционированного доступа к защищаемой информации
Владеть:
методикой выявления каналов несанкционированного доступа к информации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем	Вид занятий	Семестр / Курс	Часов	Интеракт.
	Раздел 1. Сущность и задачи обеспечения информационной безопасности в автоматизированных системах.	Раздел			
1.1	Понятие комплексной системы защиты информации. Сущность комплексной системы защиты информации. Назначение комплексной системы защиты информации.	Лек	7	4	2
1.2	Сущность и задачи обеспечения информационной безопасности в автоматизированных системах.	Лаб	7	2	0
1.3	Защита баз данных в автоматизированных системах	Ср	7	8	0
	Раздел 2. Методологические основы комплексной системы защиты информации	Раздел			
2.1	Основные понятия теории защиты информации. Методология защиты информации как теоретический базис комплексной системы защиты информации	Лек	7	4	2
2.2	Методологические основы комплексной системы защиты информации	Лаб	7	2	2
2.3	Разработка структурной модели объекта защиты	Ср	7	8	0
	Раздел 3. Определение состава защищаемой информации	Раздел			
3.1	Основные понятия теории систем	Лек	7	4	2
3.2	Определение состава защищаемой информации	Лаб	7	2	0
3.3	Разработка пространственной модели объекта защиты	Ср	7	8	0
	Раздел 4. Источники, способы и результаты дестабилизирующего воздействия на информацию	Раздел			
4.1	Методика определения состава защищаемой информации. Классификация информации по видам тайны и степеням конфиденциальности.	Лек	7	4	2

4.2	Источники, способы и результаты дестабилизирующего воздействия на информацию	Лаб	7	2	2
4.3	Моделирование способов физического проникновения	Ср	7	8	0
	Раздел 5. Каналы и методы несанкционированного доступа к информации в автоматизированных системах.	Раздел			
5.1	Определение объектов защиты. Хранилища носителей информации как объект защиты. Методы оценки защищенности предприятия	Лек	7	4	2
5.2	Каналы и методы несанкционированного доступа к информации в автоматизированных системах.	Лаб	7	2	0
5.3	Моделирование технических каналов утечки информации	Ср	7	8	0
	Раздел 6. Моделирование процессов комплексной системы защиты информации.	Раздел			
6.1	Оценка угроз безопасности информации. Явления, факторы и условия дестабилизирующего воздействия на защищаемую информацию.	Лек	7	4	2
6.2	Моделирование процессов комплексной системы защиты информации	Лаб	7	2	2
6.3	Защита корпоративного документооборота в автоматизированных системах	Ср	7	6	0
	Раздел 7. Технологическое построение комплексной системы защиты информации.	Раздел			
7.1	Источники дестабилизирующего воздействия на информацию. Виды и способы дестабилизирующего воздействия на информацию со стороны людей. Виды и способы дестабилизирующего воздействия на информацию со стороны технических средств, технологических процессов и природных явлений	Лек	7	4	0
7.2	Технологическое построение комплексной системы защиты информации	Лаб	7	2	0
7.3	Факторы, влияющие на принятие решения. Обеспечение управления КСЗИ в условиях чрезвычайных ситуаций. Подготовка мероприятий на случай возникновения чрезвычайной ситуации	Ср	7	2	0
	Раздел 8. Кадровое обеспечение комплексной системы защиты информации	Раздел			
8.1	Методика выявления каналов несанкционированного доступа к информации. Определение возможных методов несанкционированного доступа к защищаемой информации.	Лек	7	4	0
8.2	Нормативно-методическое обеспечение	Лаб	7	2	2

8.3	Понятие и основные виды чрезвычайных ситуаций. Технология принятия решения в условиях чрезвычайной ситуации.	Ср	7	2	0
	Раздел 9. Нормативно-методическое обеспечение КСЗИ.	Раздел			
9.1	Деловая разведка как канал несанкционированного доступа для получения информации. Информационный продукт как следствие реализации несанкционированных действий. Модель потенциального нарушителя	Лек	7	4	0
9.2	Планирование деятельности комплексной системы защиты информации.	Лаб	7	2	0
9.3	Цели планирования деятельности КСЗИ. Принципы планирования. Способы планирования. Основные положения разрабатываемого плана. Стадии планирования. Контроль деятельности	Ср	7	2	0
9.4	Промежуточная аттестация	Зачёт	7	2	0

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для проведения текущего контроля по дисциплине «Информационная безопасность автоматизированных систем» рассмотрены и одобрены на заседании кафедры программного обеспечения и администрирования информационных систем 30.03.2017 протокол № 8 и являются приложением к рабочей программе.

5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для проведения промежуточной аттестации по дисциплине «Информационная безопасность автоматизированных систем» рассмотрены и одобрены на заседании кафедры программного обеспечения и администрирования информационных систем 30.03.2017 протокол № 8 и являются 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
Л1.2	Артемов А. В. - Информационная безопасность: Курс лекций - Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.	http://www.iprbookshop.ru/33430	1

6.1.2. Дополнительная литература

	Заглавие	Эл. адрес	Кол-
Л2.1	Смышляев А.Г. - Информационная безопасность. Лабораторный практикум: учебное пособие - Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2015.	http://www.iprbookshop.ru/66655.html	1
Л2.2	Петров С. В., Кисляков П. А. - Информационная безопасность: Учебное пособие - Саратов: Ай Пи Ар Букс, 2015.	http://www.iprbookshop.ru/33857	1

6.1.3. Методические разработки

	Заглавие	Эл. адрес	Кол-
Л3.1	Ласкова Н. А., Емельяненко К. Э., Литвинова Е. А. - Информационная безопасность: учеб.-метод. пособие - Курск: Изд-во Курск. гос. ун-та, 2016.		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 (Проприетарная академическая лицензия)
7.3.1.8	СКЗИ "КриптоПроСР" 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 програм-ное 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 издательства «Лань» – http://e.lanbook.com/

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 Асер – 1 шт.
7.16	Жалюзи вертикальные тканевые – 1 шт.

7.17	Концентратор 24порт – 1 шт.
7.18	Лабораторный комплекс «Беспроводные сети ЭВМ»
7.19	Система активной защиты речевой акустической информации SEL-157 "Шагрень",
7.20	Устройство «Смарт (Комплекс оценки эффективности защиты речевой информации от утечки по акустическому, виброакустическому и акустоэлектрическому каналам),
7.21	Программно-аппаратные средства защиты информации от НСД .
7.22	
7.23	Помещение для самостоятельной работы обучающихся – аудитория, оснащенная компьютерной техникой 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

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

Приступая к изучению курса, студентам рекомендуется ознакомиться с содержанием рабочей программы, с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками, имеющимся на кафедре программным обеспечением и администрированием информационных систем.

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.

Самостоятельная работа студентов включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме учебной дисциплины студентам предлагается перечень заданий для самостоятельной работы.

В начале изучения курса, в учебнике или учебном пособии, рекомендуемом в качестве основной или дополнительной литературы для освоения дисциплины, студенту рекомендуется проанализировать оглавление, научно-справочный аппарат, аннотацию и предисловие.

Студенту рекомендуется использовать следующие виды записей при работе с литературой:

Конспект - краткая схематическая запись основного содержания научной работы, целью которой является не переписывание материала, а выявление его логики, системы доказательств, основных выводов. Тезисы - концентрированное изложение основных положений прочитанного материала.

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

Для изучения конспекта лекции в тот же день, после лекции студенту рекомендуется 10-15 минут.

Изучение конспекта лекции по предыдущей теме за день перед лекцией по следующей темой - 10-15 минут.

Изучение теоретического материала по учебнику и конспекту - 1 час в неделю.

Подготовка к лабораторному занятию - 30 мин.

Всего в неделю - 2 часа 55 минут.

При изучении дисциплины рекомендуется самостоятельно изучать материал, который еще не прочитан на лекции. В этом случае, понимание лекционного материала осуществляется студентом более эффективно.

Для понимания материала и качественного его усвоения рекомендуется следующая последовательность действий:

После работы на лекции, или на лабораторной работе, и после окончания учебных занятий, студенту рекомендуется самостоятельно проанализировать лекционный материал, или материал лабораторной работы (10-15 минут).

При подготовке к лекции, или лабораторной работе по следующей теме, студенту рекомендуется проанализировать лекционный материал, или материал лабораторной работы по предыдущей теме (10-15 минут).

При подготовке к лабораторным занятиям рекомендуется также изучить соответствующий теоретический материал по дисциплине, предусмотренный темой лабораторной работы.

В течение учебной недели студенту рекомендуется изучать материал по дисциплине, изложенный в рекомендуемой литературе в течение 1 часа.