

Документ подписан простой электронной подписью  
Информация о владельце:

ФИО: Худин Александр Николаевич

Должность: Ректор

Дата подписания: 26.01.2021 12:23:20

Уникальный программный ключ:

08303ad8de1c60b987361de7085acb509ac3da145741b561af0ee3e73a19

## 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 Основы управления информационной безопасностью

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация: бакалавр

Факультет физики, математики, информатики

Форма обучения: очная

Общая трудоемкость 4 ЗЕТ

Виды контроля в семестрах:  
экзамен(ы) 7

#### Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	7 (4.1)		Итого	
	18			
Неделя	уп	рп	уп	рп
Лекции	36	36	36	36
Практические	36	36	36	36
В том числе инт.	8	8	8	8
Итого ауд.	72	72	72	72
Контактная работа	72	72	72	72
Сам. работа	36	36	36	36
Часы на контроль	36	36	36	36
Итого	144	144	144	144

Рабочая программа дисциплины Основы управления информационной безопасностью / сост. кандидат педагогических наук, доцент Гранкин Валерий Егорович; Новиков Ю.М.; 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 "Основы управления информационной безопасностью" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность профиль Безопасность компьютерных систем

Составитель(и):

кандидат педагогических наук, доцент Гранкин Валерий Егорович; Новиков Ю.М.

**1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

1.1	развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности систем и их информационной инфраструктуры; развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления; привитие стремления к поиску оптимальных, простых и надежных решений
-----	---

**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:**

цели, задачи, принципы и основные направления обеспечения информационной безопасности государства

**Уметь:**

анализировать качество средств и методов защиты информационных систем

**Владеть:**

навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем

**ПК-4: Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты**

**Знать:**

основные термины по проблематике информационной безопасности

**Уметь:**

использовать комплексный подход и современные тенденции политики информационной безопасности для обеспечения защиты информации и информационных систем

**Владеть:**

полученными знаниями при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований

**4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Код занятия	Наименование разделов и тем	Вид занятий	Семестр / Курс	Часов	Интеракт.
	<b>Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации</b>	Раздел			
1.1	Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутривнутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации.	Лек	7	4	0

1.2	Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.	Лек	7	4	2
1.3	Понятие национальной безопасности	Пр	7	6	0
1.4	Роль информации-ной безопасности в обеспечении нацио-нальной безопасности государства	Ср	7	8	0
	<b>Раздел 2. Информационная война, методы и средства ее ведения</b>	Раздел			
2.1	Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.	Лек	7	4	2
2.2	Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы регио-нальной информационной безопасности.	Лек	7	4	0
2.3	Национальные ин-тересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспе-чение.	Пр	7	8	0
2.4	Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства	Ср	7	8	0
	<b>Раздел 3. Критерии защищенности компьютерных систем</b>	Раздел			
3.1	Компьютерная система как объект информационной безопасности. Общая характеристика методов и средств защиты информации. Организа-ционно-правовые, технические и криптографические методы обеспечения ин-формационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности.	Лек	7	4	2
3.2	Критерии защищенности компьютерных систем	Лек	7	4	0
3.3	Содержание информационного противоборства на межгосударственном уровне	Пр	7	8	0
3.4	Информационное оружие, его класси-фикация и возможно-сти	Ср	7	8	0
	<b>Раздел 4. Защита информации, обрабатываемой в авто-матизированных системах, от технических разведок</b>	Раздел			
4.1	Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.	Лек	7	4	2

4.2	Модели, стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Общие критерии	Лек	7	4	0
4.3	Компьютерная разведка. Технические каналы утечки информации при эксплуатации АС. Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок.	Лек	7	4	0
4.4	Содержание информации противоборства на военном уровне	Пр	7	6	0
4.5	Методы и средства обеспечения информационной безопасности компьютерных систем	Пр	7	8	0
4.6	Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.	Ср	7	8	0
4.7	Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.	Ср	7	4	0
4.8	Промежуточная аттестация	Экзамен	7	36	0

## 5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

### 5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для проведения текущего контроля по дисциплине «Основы управления информационной безопасностью» 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 «Основы управления информационной безопасностью» 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	Шаньгин В.Ф. - Информационная безопасность и защита информации: учебное пособие - Саратов: Профобразование, 2017.	<a href="http://www.iprbookshop.ru/63594.html">http://www.iprbookshop.ru/63594.html</a>	1
<b>6.1.2. Дополнительная литература</b>			
	Заглавие	Эл. адрес	Кол-
Л2.1	Шаньгин В. Ф. - Информационная безопасность и защита информации: учебное пособие - Москва: ДМК Пресс, 2014.	<a href="http://www.iprbookshop.ru/29257">http://www.iprbookshop.ru/29257</a>	1

	Заглавие	Эл. адрес	Кол-
Л2.2	Нестеров С. А. - Информационная безопасность: Учебник и практикум - М.: Издательство Юрайт, 2017.	<a href="http://www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7">http://www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7</a>	1
<b>6.1.3. Методические разработки</b>			
	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
<b>6.3.1 Перечень программного обеспечения</b>			
7.3.1.1	203:		
7.3.1.2	MacOS 10.11(Документы о приобретении iMac 21.5")		
7.3.1.3	Oracle VM VirtualBox (Свободная лицензия GNU GPL 2)		
7.3.1.4	Microsoft Windows 7 (Open License: 47818817)		
7.3.1.5	MsOffice Professional 2007 (Open Li-cense: 43219389)		
7.3.1.6	AdobeAcrobatReader DC (Бесплатное программное обеспечение)		
7.3.1.7	7-Zip (Свободная лицензия GNU LGPL)		
7.3.1.8	GoogleChrome (Свободная лицензия BSD)		
7.3.1.9	Eclipse Neon (Открытое программное обеспечение Eclipse Public License)		
7.3.1.10	VisualStudioCommunity (Проприетарная академическая лицензия)		
7.3.1.11	QtCreator 4 (Свободное программное обеспечение GPLv3)		
7.3.1.12	Code::Blocks (Свободная лицензия GNU GPLv3)		
7.3.1.13	СС КонсультантПлюс (Договор № 7/ЗЦ от 14.02.2017)		
7.3.1.14			
7.3.1.15	146:		
7.3.1.16	Microsoft Windows 7 (OpenLicense: 47818817)		
7.3.1.17	Ms OfficeProfessional 2007 (OpenLicense: 47818817)		
7.3.1.18	Google Chrome (Свободная лицензия BSD)		
7.3.1.19	7-Zip (Свободная лицензия GNU LGPL)		
7.3.1.20	Adobe Acrobat Reader DC (Бесплатное программное обеспечение )		
<b>6.3.2 Перечень информационных справочных систем</b>			
7.3.2.1	Каталог библиотеки КГУ. - Режим доступа: <a href="http://195.93.165.10:2280">http://195.93.165.10:2280</a>		
7.3.2.2	Электронная библиотека. - Режим доступа: <a href="http://elibrary.ru">http://elibrary.ru</a>		
7.3.2.3	Университетская информационная система «Россия» – <a href="http://uisrussia.msu.ru">http://uisrussia.msu.ru</a>		
7.3.2.4	Электронная библиотечная система «КнигаФонд» – <a href="http://www.knigafund.ru/">http://www.knigafund.ru/</a>		
7.3.2.5	Электронная библиотечная система издательства «Лань» – <a href="http://e.lanbook.com/">http://e.lanbook.com/</a>		

## 7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Компьютерная аудитория: учебная аудитория для проведения за-нятий лекционного типа, занятий семинарского типа, курсового проектирования, групповых и индивидуальных консультаций, те-кущего контроля и промежуточной аттестации,		
7.2	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 203.		
7.3	Комплекты учебных столов и стульев (10 шт),		
7.4	комплекты компьютерных столов и стульев (15 шт)		
7.5	Жалюзи вертикальные тканевые – 14 шт.		

7.6	Apple iMac 21.5 – 15 шт.
7.7	Концентратор 16-портовый – 1 шт.
7.8	
7.9	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.
7.10	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 146.
7.11	Столов – 61
7.12	Посадочных мест – 162
7.13	Компьютеров:
7.14	Для пользователей – 40
7.15	Для библиотекаря – 2
7.16	Моноблоков MSI (27 ) - модель MS-A912, 2Gb оперативной памяти, Athlon CPU D525 1.80GHz
7.17	Моноблоков Asus (13) - модель ET2220I, 4Gb 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 практическому 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 практической работе, и после окончания учебных занятий, студенту рекомендуется самостоятельно проанализировать лекционный материал, или материал практической работы (10-15 минут).

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

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

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