МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г. ШУХОВА»
(БГТУ им. В.Г. Шухова)

УТВЕРЖДАЮ
Директор института
_____
«11» 12 2015 г.

РАБОЧАЯ ПРОГРАММА

дисциплины (модуля)

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(наименование дисциплины, модуля)

направление подготовки (специальность):

27.03.04 – Управление в технических системах
(шифр и наименование направления бакалавриата, магистра, специальности)

Направленность программы (профиль, специализация):

27.03.04 – 01 – Управление в технических системах (промышленность)
(наименование образовательной программы (профиль, специализация)

Квалификация

бакалавр
(бакалавр, магистр, специалист)

Форма обучения

очная
(очная, заочная и др.)

Институт: Информационных технологий и управляющих систем

Кафедра: Технической кибернетики

Белгород – 2015

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования 27.03.04 – Управление в технических системах (бакалавриат), приказ Минобрнауки России от 20 октября 2015 г. №1171,
- плана учебного процесса БГТУ им. В.Г. Шухова, введенного в действие в 2015 году по направлению подготовки 27.03.04 – Управление в технических системах (бакалавриат).

Составитель (составители): к.т.н. _____ (А.Г. Бажанов)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа согласована с выпускающей кафедрой
техническая кибернетика
(наименование кафедры)

Заведующий кафедрой: д.т.н., проф. _____ (В.Г. Рубанов)
(ученая степень и звание, подпись) (инициалы, фамилия)

«11» 12 2015 г.

Рабочая программа обсуждена на заседании кафедры

«11» 12 2015 г., протокол № 4

Заведующий кафедрой: д.т.н., проф. _____ (В.Г. Рубанов)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа одобрена методической комиссией института

«11» 12 2015 г., протокол № 4

Председатель: к.т.н., доц. _____ (Ю.И. Солопов)
(ученая степень и звание, подпись) (инициалы, фамилия)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Формируемые компетенции			Требования к результатам обучения
№	Код компетенции	Компетенция	
Профессиональные			
1	ПК-1	Способность выполнять эксперименты на действующих объектах по заданным методикам и обрабатывать результаты с применением современных информационных технологий и технических средств	В результате освоения дисциплины обучающийся должен **Знать:** задачи информационной безопасности; уровни формирования режима информационной безопасности; особенности законодательно-правового и административного уровней; основное содержание оценочного стандарта ISO/IEC 15408; основное содержание стандартов по информационной безопасности распределенных систем; основные сервисы безопасности в вычислительных сетях; наиболее эффективные механизмы безопасности; цели и задачи административного уровня обеспечения информационной безопасности; содержание административного уровня; классы угроз информационной безопасности; причины и источники случайных воздействий на информационные системы; каналы несанкционированного доступа к информации; основные угрозы для безопасности информации; методы построения безопасных информационных структур и способы их анализа. **Уметь**: использовать стандарты для оценки защищенности информационных систем; выбирать механизмы безопасности для защиты распределенных вычислительных сетей; определять классы защищенных систем по совокупности мер защиты; выявлять и классифицировать угрозы информационной безопасности; пользоваться программными средствами, реализующими основные криптографические функции: системы публичных ключей, цифровую подпись, разделение доступа. **Владеть:** навыками применения методов оценки и анализа вероятных угроз информационной безопасности объекта; навыками обеспечения защиты информации, составляющей государственную тайну и иной служебной информации; программными и аппаратными средствами защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Содержание дисциплины основывается и является логическим продолжением следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Операционные системы
2	Информационные системы
3	Программирование и основы алгоритмизации

Содержание дисциплины служит основой для изучения следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Проектирование систем управления
2	Программирование АСУ

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 зач. единицы, 108 часов.

Вид учебной работы	Всего часов	Семестр №6
Общая трудоемкость дисциплины, час	108	108
Контактная работа (аудиторные занятия), в т.ч.:	34	34
лекции	17	17
лабораторные	17	17
практические		
Самостоятельная работа студентов, в том числе:	74	74
Курсовой проект		
Курсовая работа		
Расчетно-графическое задания		
Индивидуальное домашнее задание		
Другие виды самостоятельной работы:	74	74
Самостоятельная работа при подготовке к экзамену	38	38
Самостоятельная работа при подготовке к лабораторным занятиям	17	17
Самостоятельная работа при подготовке к лекциям	17	17
Форма промежуточная аттестация (зачет, экзамен)	36	36

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Наименование тем, их содержание и объем

Курс 3 Семестр 6

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час

		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
1.	Введение в основы информационной безопасности. Основные понятия, термины, используемые обозначения				
	Понятие информационной безопасности. Проблема информационной безопасности общества. Достоверность, целостность и конфиденциальность информации. Задачи информационной безопасности общества. Уровни систем безопасности.	1			1
2.	Основы государственной информационной политики и информационной безопасности				
	Нормативно-правовые основы информационной безопасности в РФ. Ответственность за нарушения в сфере информационной безопасности. Стандарты информационной безопасности. Безопасность распределенных систем. Концепция национальной безопасности РФ.	2			2
3.	Проблемы информационной безопасности в сфере управления				
	Компьютерные вирусы и возможности защиты. Описание аппаратно-программных средств, способствующих распространению и уничтожению вирусных составляющих. Классификация вирусов. Открытость систем управления для угроз.	2		4	6
4.	Информационная безопасность автоматизированных систем. Организационно-правовое обеспечение информационной безопасности				
	Принципы организации обмена данными в автоматизированных системах. Функциональное программное обеспечение, используемое при проектировании и работе систем управления. Доктрина информационной безопасности. Стандарты для защиты информационно-управляющих систем и сетей от воздействия угроз несанкционированного доступа и заражения.	2			2
5.	Основные угрозы информации				
	Способы вмешательства в информационные системы предприятия. Нарушение работы автоматизированных систем управления путем перехвата сообщений. Инъекции вредоносного кода в управляющие программы.	2			2
6.	Информационные системы современного предприятия				
	Иерархия современных информационных систем предприятия. Оценка уязвимости каждого из уровней.	2			2
7.	Методы и модели оценки уязвимости информации и их анализ				
	Моделирование вероятности внедрения злоумышленника в системы управления. Оценка последствий атаки на сеть предприятия.	1			1
8.	Функции, задачи и стратегии защиты информации				
	Методика создания безопасных систем на производстве. Идентификация и аутентификация для управляющего и сетеобразующего оборудования.	1			1

9. Криптографические методы защиты информации					
	Криптография и шифрование. Методы шифрования и способы их взлома. Оценка затрат вычислительного времени на обработку защищенной информации. Электронная цифровая подпись и ее возможности.	2		8	10
10. Архитектура систем защиты информации					
	Описание безопасных структур управления для опасных производств. Методы разграничения доступа. Резервирование и дублирование. Экранирование. Необходимые элементы систем управления для защиты. Виртуальные частные сети.	2		5	7
	ВСЕГО	17		17	34

4.2. Содержание практических (семинарских) занятий
(Не предусмотрены)

4.3. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	К-во часов СРС
семестр № 7				
1	Проблемы информационной безопасности в сфере управления	Создание и тестирование программы для простейших способов взлома файлов с паролем	4	4
2	Криптографические методы защиты информации	Изучение методов шифрования и оценка их стойкости	4	4
3	Криптографические методы защиты информации	Создание модели для оценки стойкости криптографических алгоритмов	4	4
4	Архитектура систем защиты информации	Изучение структур систем управления с защитой от кибернетических угроз	5	5
		ИТОГО:	17	17
			ВСЕГО:	34

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

5.1. Перечень контрольных вопросов (типовых заданий)

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1.	Введение в основы информационной безопасности. Основные понятия, термины, используемые обозначения	1. Понятие и виды информации. 2. Проблема информационной безопасности общества. 3. Достоверность, целостность и конфиденциальность информации. 4. Задачи информационной безопасности общества. 5. Уровни систем безопасности.

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
2.	Основы государственной информационной политики и информационной безопасности	6. Правовая основа обеспечения информационной безопасности. 7. Основные положения Доктрины информационной безопасности Российской Федерации. 8. Государственная политика обеспечения информационной безопасности Российской Федерации 9. Нормативно-правовые основы информационной безопасности в РФ. 10. Ответственность за нарушения в сфере информационной безопасности. 11. Стандарты информационной безопасности. 12. Безопасность распределенных систем. 13. Концепция национальной безопасности РФ.
3.	Проблемы информационной безопасности в сфере управления	14. Понятие защиты информации и виды защиты информации. 15. Способы несанкционированного доступа к автоматизированным системам
4.	Информационная безопасность автоматизированных систем. Организационно-правовое обеспечение информационной безопасности	16. Защита информации, составляющей государственную тайну. 17. Способы защиты информации
5.	Основные угрозы информации	18. Угрозы информационной безопасности. 19. Виды каналов утечки информации. 20. Угрозы безопасности информации, обрабатываемой в автоматизированных системах. 21. Объективные факторы, представляющие угрозу безопасности информации. 22. Субъективные факторы, представляющие угрозу безопасности информации.
6.	Информационные системы современного предприятия	23. Иерархия подсистем современного промышленного предприятия. 24. Оценка уровня угроз на каждом этапе.
7.	Методы и модели оценки уязвимости информации и их анализ	25. Классификация средств защиты информации. 26. Моделирование оценки уязвимости на основе расчетных данных
8.	Функции, задачи и стратегии защиты информации	27. Основные принципы и направления защиты автоматизированных систем от несанкционированного доступа. 28. Виды технических средств защиты информации. 29. Идентификация пользователя и аутентификация электронного сообщения

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
9.	Криптографические методы защиты информации	30. Криптография как наука, симметричные и несимметричные алгоритмы шифрования. 31. Классификация методов шифрования информации. 32. Криптография и стеганография. Особенности и отличия. 33. Программные средства шифрации и защиты информации. 34. Понятие электронной цифровой подписи (ЭЦП), управление ключами.
1.	Архитектура систем защиты информации	35. Методы ограничения доступа к информации. 36. Создание комплексной системы защиты информации.

5.2. Перечень тем курсовых проектов, курсовых работ, их краткое содержание и объем

(Не предусмотрены)

6. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

6.1. Перечень основной литературы

1) Бабаш, А.В. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А. В. Бабаш. – 2-е изд. – М.: ИЦ РИ0Р: НИЦ ИНФРА-М, 2014. – 216 с.
2) Малюк, А.А. Введение в защиту информации в автоматизированных системах: учеб. пособие / А. А. Малюк, С. В. Пазинин, Н. С. Погожин. – 3-е изд., стер. – М: Горячая линия – Телеком, 2005. – 144 с.
3) Хорев, П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие для студентов вузов, обучающихся по направлению 230100 (654600) / П. Б. Хорев. – 4-е изд., стер. – М: Академия, 2008. – 256 с.
4) Хорев, П.Б. Криптографические интерфейсы и их использование / П. Б. Хорев. – М: Горячая линия - Телеком, 2007. – 278 с.
5) Денисов, И.А. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс] / И.А. Денисов – Электрон. текстовые данные. – М: Московский технический университет связи и информатики, 2016. – 31 с. – Режим доступа: http://www.iprbookshop.ru/61529.html.
6) Шаньгин, В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф. – Электрон. текстовые данные. – М: ДМК Пресс, 2014. – 702 с. – Режим доступа: http://www.iprbookshop.ru/29257.
7) Башлы, П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / Башлы П.Н., Бабаш А.В., Баранова Е.К. – Электрон. текстовые данные. – М: Евразийский открытый институт, 2012. – 311 с. – Режим доступа: http://www.iprbookshop.ru/10677.html.

6.2. Перечень дополнительной литературы

1) Зубов, А.Ю. Криптографические методы защиты информации. Совершенные шифры: учеб. пособие / А. Ю. Зубов. – М: Гелиос АРВ, 2005. – 190 с.

2) Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П.А. Тимофеев, В. Ф. Шаньгин. – М: Радио и связь, 1999. – 328 с.
3) Мельников, В.В. Безопасность информации в автоматизированных системах / В.В. Мельников. – М: Финансы и статистика, 2003. – 367 с.
4) Храмцов, Б.А. Мониторинг промышленной безопасности: учеб. пособие для студентов заоч. формы обучения с применением дистанц. технологий специальности 280102 (330500) / Б.А. Храмцов, Е.В. Климова, А.А. Ростовцева. – Белгород: Изд-во БГТУ им. В.Г. Шухова, 2008. – 343 с.
5) Аверченков, В.И. Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.]. – Электрон. текстовые данные. – Брянск: Брянский государственный технический университет, 2012. – 187 с. – Режим доступа: http://www.iprbookshop.ru/7000.html.
6) Васильев, В.И. Интеллектуальные системы защиты информации. [Электронный ресурс] – Электрон. дан. – М: Машиностроение, 2013. – 172 с. – Режим доступа: http://e.lanbook.com/book/5792.
7) Горбунов, В.А. Математические методы в теории защиты информации. [Электронный ресурс] – Электрон. дан. – М: Горная книга, 2004. – 82 с. – Режим доступа: http://e.lanbook.com/book/3490.
8) Голиков, А.М. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Голиков А.М. – Электрон. текстовые данные. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2007. – 288 с. – Режим доступа: http://www.iprbookshop.ru/13957.html.

6.3. Перечень интернет ресурсов

http://www.elibrary.ru- Научная электронная библиотека

http://www.gpntb.ru/- Государственная публичная научно-техническая библиотека России

http://elibrary. bmstu./ru – Библиотека МГТУ им. Н.Баумана

http://www.viniti.ru – Всероссийский институт научной информации по техническим наукам(ВИНИТИ)

http://www.unilib.neva.ru/rus/- Фундаментальная библиотека Санкт-Петербургского государственного политехнического университета

http://elibrary.eltech.ru – Библиотека Санкт-Петербургского государственного электротехнического университета

http://www.ntb.bstu.ru и переход к системе NormaCS - Электронно-библиотечная система БГТУ им В.Г.Шухова

7.МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Преподавание дисциплины «Основы информационной безопасности» осуществляется в следующих аудиториях:

1) специализированный компьютерный класс МК229: 15 персональных компьютеров с выходом в интернет, проектор, 10 комплектов оборудования для моделирования систем Matlab;

при активном использовании ИКТ, используя в учебном процессе для улучшения наглядности и доступности следующее обеспечение:

- мультимедиа и анимационный материал поясняющее работу элементов и устройств;
- презентационное программное обеспечение для демонстрации презентаций по разнообразным темам;
- MathWorks Individual Licenses (per License): MATLAB 2016b, Simulink, Neural Networks Toolbox, Fuzzy Logic Toolbox, Control System Toolbox 10 бессрочная лиц. №1145851;
- MathWorks Individual Licenses (per License): MATLAB 2014b, Simulink, Neural Networks Toolbox, Statistics and Machine Learning Toolbox10 бессрочная лиц. №362444;
- Microsoft Windows 7 64x MSDN подписка БГТУ;
- Microsoft Office 2013 лицензия БГТУ.

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2016/2017 учебный год.

Протокол № 10 заседания кафедры от «16» 05 2016г.

Заведующий кафедрой _____ Рубанов В.Г.
подпись, ФИО

Директор института _____ Белоусов А.В.
подпись, ФИО

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2017/2018 учебный год.
Протокол № 11 заседания кафедры от «15» 05 2017г.

Заведующий кафедрой _____ Рубанов В.Г.
подпись, ФИО

Директор института _____ Белоусов А.В.
подпись, ФИО

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2018/2019 учебный год.

Протокол № 13 заседания кафедры от «01» 06 2018г.

Заведующий кафедрой _____ Рубанов В.Г.

подпись, ФИО

Директор института _____ Белоусов А.В.

подпись, ФИО

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2019/2020 учебный год.

Протокол № 12 заседания кафедры от «17» 05 2019 г.

Заведующий кафедрой _____

подпись, ФИО

Директор института _____

подпись, ФИО

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2020/2021 учебный год.

Протокол № 10 заседания кафедры от «28» 05 2020г.

Заведующий кафедрой _____

подпись, ФИО

Директор института _____

подпись, ФИО

ПРИЛОЖЕНИЯ

Приложение №1. Методические указания для обучающегося по освоению дисциплины (включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине).

Данный курс состоит из лекций и лабораторных работ. Основой является модульный метод обучения, сущность которого состоит в том, что содержание обучения структурируется в автономные организационно-методические блоки – модули, содержание и объём которых могут варьировать в зависимости от дидактических целей. Сами модули формируются в виде разделов, объединяемых по тематическому признаку.

Информационные технологии предполагают использование электронных материалов, системных и программных средств. Применение персональных компьютеров при изучении дисциплины активизирует познавательную деятельность студентов в области современных информационных технологий.

Самостоятельная работа студентов предполагает активное, последовательное и подробное освоение ими соответствующих учебных материалов дисциплины по всем ее структурным разделам с использованием рекомендуемой основной и дополнительной литературы и интернет источников. При рассмотрении всех разделов дисциплины рекомендуется постоянная работа с Интернет-ресурсами, с вебинарами проводимыми на русском и английском языках. Итоговый контроль осуществляется в форме зачета после изучения всех частей курса.