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 ИТУС
_____ В.Г. Рубанов
«__» _____ 2016 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Основы информационной безопасности

Направление подготовки:
09.03.01 Информатика и вычислительная техника

профиль подготовки:

Вычислительные машины, комплексы, системы и сети

Квалификация (степень)
бакалавр

Форма обучения
очная

Институт Информационных технологий и управляющих систем

Кафедра Программного обеспечения вычислительной техники и автоматизированных систем

Белгород – 2016

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.01 «Информатика и вычислительная техника» (уровень бакалавриата), утверждённого приказом Министерства образования и науки Российской Федерации № 5 от 12 января 2016 г.
- плана учебного процесса БГТУ им. В. Г. Шухова по направлению подготовки 09.03.01 «Информатика и вычислительная техника», профиль «Вычислительные машины, комплексы, системы и сети».

Составитель: _____ (И. Н. Гвоздевский)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа согласована с выпускающей кафедрой
Программного обеспечения вычислительной техники и автоматизированных систем

Заведующий кафедрой: к.т.н., доцент _____ (В. М. Поляков)
(подпись) (инициалы, фамилия)

« 11 » 03 2016 г.

Рабочая программа обсуждена на заседании кафедры
Программного обеспечения вычислительной техники и автоматизированных систем

« 11 » 03 2016 г., протокол № 7

Заведующий кафедрой: к.т.н., доцент _____ (В. М. Поляков)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа одобрена методической комиссией института
Информационных технологий и управляющих систем

« 24 » 03 2016 г., протокол № 7

Председатель: к.т.н., доцент _____ (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	
Общепрофессиональные			
1	ОПК-5	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	В результате освоения дисциплины обучающийся должен **Знать:** основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; принципы формирования политики информационной безопасности в автоматизированных системах. **Уметь:** применять средства обеспечения безопасности данных; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;

			разрабатывать частные политики информационной безопасности автоматизированных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем. **Владеть:** навыками организации и обеспечения режима секретности; методами организации и управления деятельностью служб защиты информации на предприятии; методами формирования требований по защите информации.
Профессиональные			
1	ПК-2	способность разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования	В результате освоения дисциплины обучающийся должен **Знать:** основные средства обеспечения информационной безопасности **Уметь:** применять средства обеспечения безопасности данных при разработке компонент аппаратно-программных комплексов и баз данных. **Владеть:** навыками разработки компонентов аппаратно-программных комплексов и баз данных с учетом требований информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Содержание дисциплины основывается и является логическим продолжением следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Информатика

Содержание дисциплины служит основой для изучения следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Программно-аппаратные средства обеспечения информационной безопасности
2	Администрирование распределенных вычислительных систем

3. ОБЪЕМ ДИСЦИПЛИНЫ

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

Вид учебной работы	Всего часов	Семестр № 5
Общая трудоемкость дисциплины, час	108	108
Контактная работа (аудиторные занятия), в т.ч.:	51	51
лекции	17	17
лабораторные	34	34
практические		
Самостоятельная работа студентов, в том числе:	57	57
Курсовой проект		
Курсовая работа		
Расчетно-графическое задания		
Индивидуальное домашнее задание	9	9
Другие виды самостоятельной работы	48	48
Форма промежуточная аттестация (зачет, экзамен)	Зачет	Зачет

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Наименование тем, их содержание и объем

Курс 3 Семестр 5

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
1.					
	Понятие национальной безопасности, виды безопасности. Информационная безопасность в системе национальной безопасности Российской Федерации.	2		2	4
2.					

	Терминологические основы информационной безопасности. Основные понятия и определения. Конфиденциальность, целостность, доступность	2		4	7
3.					
	Общеметодологические принципы теории информационной безопасности. Комплексность. Этапы развития информационной безопасности: Системы безопасности ресурса; Этап развитой защиты; Этап комплексной защиты. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Комплексность: целевая, инструментальная, структурная, функциональная, временная.	3		6	9
4.					
	Угрозы. Классификация и анализ угроз информационной безопасности. подверженность физическому искажению или уничтожению; возможность несанкционированной (случайной или злоумышленной) модификации; опасность несанкционированного получения информации лицами, для которых она не предназначена. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные.	3		8	10
5.					
	Методы и средства обеспечения информационной безопасности. Методы нарушения конфиденциальности, целостности и доступности информации. Причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные непреднамеренные. Потенциально возможные злоумышленные действий в автоматизированных системах обработки данных.	3		6	8
6.					

	Функции и задачи защиты информации. Методы формирования функций защиты. Скрытие информации о средствах, комплексах, объектах и системах обработки информации. Дезинформация противника. Легендирование. Введение избыточности элементов системы. Резервирование элементов системы. Регулирование доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации. Маскировка информации. Регистрация сведений. Уничтожение информации. Обеспечение сигнализации. Обеспечение реагирования. Управление системой защиты информации. Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека. Применение криптографии.	4		8	10
	ВСЕГО	17		34	48

4.2. Содержание практических (семинарских) занятий

Учебным планом не предусмотрены.

4.3. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	К-во часов СРС
семестр № 5				
1	Понятие национальной безопасности, виды безопасности. Информационная безопасность в системе национальной безопасности Российской Федерации.	Роль информационной безопасности в современном обществе	4	4
2	Терминологические основы информационной безопасности. Основные понятия и определения. Конфиденциальность, целостность, доступность	Информационное противодействие. Информационные войны. Кибер атаки	4	4
3	Общеметодологические принципы теории информационной безопасности.	Разработка документации согласно требованиям стандартов и ГОСТов.	6	6

	Комплексность.			
4	Угрозы. Классификация и анализ угроз информационной безопасности.	Вредоносное программное обеспечение и методы борьбы	6	6
5	Методы и средства обеспечения информационной безопасности.	Интернет угрозы и методы борьбы с ними.	6	6
6	Функции и задачи защиты информации. Методы формирования функций защиты.	Современные системы управления информационной безопасностью	4	4
7	Функции и задачи защиты информации. Методы формирования функций защиты.	Электронно-цифровая подпись. Система удостоверяющих центров. Сертификаты.	4	4
		ИТОГО:	34	34
			ВСЕГО:	68

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	Понятие национальной безопасности, виды безопасности. Информационная безопасность в системе национальной безопасности Российской Федерации.	1. Доктрина безопасности РФ. 2. Национальные и международные документы в области защиты информации. 3. Физическая защита информационных систем. 4. Программные средства защиты информации. 5. Этапы создания систем защиты информации. 6. Защита информации. Основные принципы обеспечения информационной безопасности. 7. Доктрина информационной безопасности РФ. ГОСТЫ РФ. 8. Информация. Виды информации, свойства и понятие информации в контексте информационной безопасности.
2	Терминологические основы информационной безопасности. Основные понятия и определения. Конфиденциальность, целостность, доступность	1. Требования по защите ИС и классы защиты ИС. 2. Положение о защите информации. 3. Безопасность глобальных сетевых технологий и методы информационного воздействия на глобальные информационные сети. 4. Правовые основы защиты информации и

		закон о защите информации.
3	Общеметодологические принципы теории информационной безопасности. Комплексность.	1. Защита информации. Основные принципы обеспечения информационной безопасности. 2. Доктрина информационной безопасности РФ. ГОСТЫ РФ. 3. Информация. Виды информации, свойства и понятие информации в контексте информационной безопасности.
4	Угрозы. Классификация и анализ угроз информационной безопасности.	1. Биометрия. Технологии создания защищенных систем с помощью биометрии. 2. Угрозы, виды угроз и дифференциация угроз. 3. Методы несанкционированного доступа в локальные сети. 4. Модель нарушителя. 5. Угрозы. Классификация угроз. Активные и пассивные угрозы. 6. Спам. Защита от спама. Средства и технологии защиты от спама.
5	Методы и средства обеспечения информационной безопасности.	1. Правовые основы защиты информации и закон о защите информации. 2. ЭЦП. Роль ЭЦП в современном обществе. Технология ЭЦП. 3. Международные документы и стандарты в области информационной безопасности. 4. Классы каналов несанкционированного получения информации 5. Основные свойства информации. Важность, полнота, адекватность, релевантность
6	Функции и задачи защиты информации. Методы формирования функций защиты.	1. Антивирусы и антивирусная защита. Классификация вредоносных программ. 2. Межсетевые экраны и методы создания защищенных систем включающих межсетевые экраны. 3. Особенности защиты различных операционных систем. 4. Аппаратные средства защиты информации. 5. Протоколы PPP, SMTP, FTP и методы создания защищенного обмена 6. Что такое информация? 7. Понятие информационной безопасности. 8. Обеспечение безопасности при работе с электронной почтой. 9. Резервирование информации. Средства

		создания резервных копий. 10. Что такое «криптография»? 11. Физическое разрушение информационных систем и методы защиты от физического воздействия. 12. Троянские кони, люки и технология салями. 13. Технология VPN. Построение защищенных каналов связи. 14. Сертификаты. Протокол HTTPS. Центры сертификации. 15. Понятие информации в контексте информационной безопасности. 16. Виды информации. 17. Что такое «СПАМ»? 18. Информационные системы, использующие технологии ЭЦП

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

Учебным планом не предусмотрены.

5.3. Перечень индивидуальных домашних заданий, расчетно-графических заданий.

Темы для подготовки рефератов в виде индивидуальных домашних заданий:

1. Правовые основы защиты информации и закон о защите информации.
2. ЭЦП. Роль ЭЦП в современном обществе. Технология ЭЦП.
3. Международные документы и стандарты в области информационной безопасности.
4. Классы каналов несанкционированного получения информации
5. Основные свойства информации. Важность, полнота, адекватность, релевантность
6. Доктрина безопасности РФ.
7. Национальные и международные документы в области защиты информации.
8. Физическая защита информационных систем.
9. Программные средства защиты информации.
10. Этапы создания систем защиты информации.
11. Защита информации. Основные принципы обеспечения информационной безопасности.
12. Доктрина информационной безопасности РФ. ГОСТЫ РФ.
13. Информация. Виды информации, свойства и понятие информации в контексте информационной безопасности.
14. Антивирусы и антивирусная защита. Классификация вредоносных

программ.

15. Межсетевые экраны и методы создания защищенных систем, включающих межсетевые экраны.
16. Особенности защиты различных операционных систем.
17. Аппаратные средства защиты информации.
18. Протоколы PPP, SMTP, FTP и методы создания защищенного обмена
19. Обеспечение безопасности при работе с электронной почтой.
20. Резервирование информации. Средства создания резервных копий.
21. Что такое «криптография»?
22. Физическое разрушение информационных систем и методы защиты от физического воздействия.
23. Троянские кони, люки и технология салями.
24. Технология VPN. Построение защищенных каналов связи.
25. Сертификаты. Протокол HTTPS. Центры сертификации.
26. Понятие информации в контексте информационной безопасности.
27. Виды информации.
28. Что такое «СПАМ»?
29. Информационные системы, использующие технологии ЭЦП

5.4. Перечень контрольных работ.

Учебным планом не предусмотрены.

6. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

6.1. Перечень основной литературы

1. Белов Е.Б. Основы информационной безопасности: учебное пособие – Горячая линия – Телеком, 2011.
2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства: Учебное пособие – М.: ДМК Пресс, 2010.
3. А.П. Курило [и др.] Основы управления информационной безопасностью: учебное пособие – М.: Горячая линия – Телеком, 2012. http://www.iprbookshop.ru/12021
4. Сычев Ю.Н. Основы информационной безопасности : учебно-методический комплекс – М.: Евразийский открытый институт, 2012. http://www.iprbookshop.ru/14642
5. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2010.— 544 с.— Режим доступа: http://www.iprbookshop.ru/7943.— ЭБС «IPRbooks», по паролю
6. Белов Е.Б. Основы информационной безопасности: учебное пособие – Горячая линия – Телеком, 2011. http://www.iprbookshop.ru/12014.html
7. Нестеров С.А. Основы информационной безопасности: Учебное пособие – Санкт-Петербургский политехнический университет Петра Великого, 2014.

6.2. Перечень дополнительной литературы

1. Малюк А.А. Введение в информационную безопасность: Учебное пособие – М.: Горячая линия - Телеком , 2011.
2. Малюк А.А. Введение в информационную безопасность [Электронный ресурс]: учебное пособие/ Малюк А.А., Горбатов В.С., Королев В.И.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2011.— 288 с.— Режим доступа: http://www.iprbookshop.ru/11979.— ЭБС «IPRbooks», по паролю
3. Основы управления информационной безопасностью [Электронный ресурс]: учебное пособие/ А.П. Курило [и др.].— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 244 с.— Режим доступа: http://www.iprbookshop.ru/12021.— ЭБС «IPRbooks», по паролю
4. Сычев Ю.Н. Основы информационной безопасности [Электронный ресурс]: учебно-методический комплекс/ Сычев Ю.Н.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 342 с.— Режим доступа: http://www.iprbookshop.ru/14642.— ЭБС «IPRbooks», по паролю

6.3. Перечень интернет ресурсов

1. Библиотека TechNet [Электронный ресурс]. – Режим доступа: http://technet.microsoft.com/ru-ru/library/aa991542
2. Библиотека OsZone [Электронный ресурс]. – Режим доступа: http://www.oszone.net/1/Windows
3. Форум информационной безопасности SecurityLab | Уязвимости [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/vulnerability/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Учебные аудитории для проведения занятий лекционного типа, лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации.

Для освоения дисциплины могут быть использованы программные средства:

1. Microsoft Office;
2. Microsoft Windows;
3. Kaspersky Endpoint Security 10 для Windows;
4. Microsoft Windows Server WSUS;
5. XSpider Education;
6. MaxPatrol SIEM Education;
7. MaxPatrol Education;
8. Positive Technologies Application Firewall Educstion.

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

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

Протокол № 12 заседания кафедры от «20» 06 2016 г.

Заведующий кафедрой _____ В.М. Поляков
подпись ФИО

Директор института _____ А.В. Белоусов

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2017/2018 учебный год.

Протокол № 11 заседания кафедры от «22» 05 2017 г.

Заведующий кафедрой _____ В.М. Поляков
подпись, ФИО

Директор института _____ А.В. Белоусов

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

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

Протокол № 10 заседания кафедры от «21» 05 2019 г.

Заведующий кафедрой _____ В.М. Поляков
подпись, ФИО

Директор института _____ А.В. Белоусов

ПРИЛОЖЕНИЯ

Приложение №1.

Методические указания для обучающегося по освоению дисциплины

Курс «Основы информационной безопасности» является базовым для подготовки студентов специальности 09.03.01 Информатика и вычислительная техника.

Целью курса является изучение основных понятий информационной безопасности, которые понадобятся для дальнейшего обучения.

В ходе изучения дисциплины студенты приобретают практические навыки и умения:

Классификации угроз в информационных системах ;

Анализа состояний информационных систем;

Создания регламентов, описывающих поведение объектов для обеспечения безопасности;

Занятия проводятся в виде лекций и лабораторных работ в соответствии с рабочей программой. Для изучения курса большое значение имеет самостоятельная работа студентов.

Формы контроля знаний студентов предполагают текущий и итоговый контроль. Текущий контроль знаний проводится в устного опроса. Формой итогового контроля является зачет.

Перед итоговым контролем рекомендуется проводить консультации, в том числе, по необходимости — индивидуальные.

Самостоятельная работа является главным условием успешного освоения изучаемой учебной дисциплины.

Исходный этап изучения курса предполагает ознакомление с рабочей программой, характеризующей границы и содержание учебного материала, который подлежит освоению.

Изучение отдельных тем курса необходимо осуществлять в соответствии с поставленными в них целями, их значимостью, основываясь на содержании и вопросах, поставленных в лекции преподавателя и приведенных в планах и заданиях к практическим занятиям, а также методических указаниях для студентов заочного обучения.

В учебниках и учебных пособиях, представленных в списке рекомендуемой литературы содержатся возможные ответы на поставленные вопросы. Инструментами освоения учебного материала являются основные термины и понятия, составляющие категориальный аппарат дисциплины. Их осмысление, запоминание и практическое использование являются обязательным условием овладения курсом.

Изучение каждой темы следует завершать выполнением лабораторных заданий, ответами на тесты, решением задач, содержащихся в соответствующих разделах учебников и методических пособий. Для обеспечения систематического контроля над процессом усвоения тем курса следует пользоваться перечнем контрольных вопросов для проверки знаний по дисциплине, содержащихся в планах и заданиях к практическим занятиям и методическим указаниях для студентов заочного отделения. Если при ответах на сформулированные в перечне

вопросы возникнут затруднения, необходимо очередной раз вернуться к изучению соответствующей темы, либо обратиться за консультацией к преподавателю.

Успешное освоение курса дисциплины возможно лишь при систематической работе, требующей глубокого осмысления и повторения пройденного материала, поэтому необходимо делать соответствующие записи по каждой теме.

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

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

Протокол № 10 заседания кафедры от «18» мая 2019 г.

Заведующий кафедрой _____ В.М. Поляков
подпись, ФИО

Директор института _____ А.В. Белоусов

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений
Рабочая программа без изменений утверждена на 2020/2021 уч. год.

Протокол № 8 заседания кафедры от «21» 04 2020 г.

Заведующий кафедрой _____ Поляков В.М.
подпись, ФИО

Директор института _____ Белоусов А.В.
подпись, ФИО

7. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ[1]

Рабочая программа утверждена на 2021/2022 учебный год без изменений[2]

Протокол № 8 заседания кафедры от « 15 » мая 2021 г.

Заведующий кафедрой _____ Поляков В.М.
подпись, ФИО

Директор института _____ Белоусов А.В.
подпись, ФИО

[1] Заполняется каждый учебный год на отдельных листах
[2] Нужное подчеркнуть