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 энергетики, информационных технологий и управляющих систем
_____ Белоусов А.В.
«20» 12 2021 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Управление информационной безопасностью

направление подготовки:

10.05.03 Информационная безопасность автоматизированных систем

Специализация программы:

Безопасность открытых информационных систем

Квалификация

Специалист по защите информации

Форма обучения

очная

Институт энергетики, информационных технологий и управляющих систем

Кафедра Программного обеспечения вычислительной техники и автоматизированных систем

Белгород 2021

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Минобрнауки России от 26.11.2020 №1457
- учебного плана, утвержденного ученым советом БГТУ им. В.Г. Шухова в 2021 году.

Составитель: к.т.н., доцент _____ (Гаврющенко А.П.)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа обсуждена на заседании кафедры

«14» 05 2021 г., протокол № 8

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

Рабочая программа согласована с выпускающей кафедрой программного обеспечения вычислительной техники и автоматизированных систем
(наименование кафедры/кафедр)

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

«14» 05 2021 г.

Рабочая программа одобрена методической комиссией института

«20» 05 2021 г., протокол № 9

Председатель к.т.н., доцент _____ (Семернин А.Н.)
(ученая степень и звание, подпись) (инициалы, фамилия)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Категория (группа) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Наименование показателя оценивания результата обучения по дисциплине
Общепрофессиональные компетенции	ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1 Применяет нормативные правовые акты, регламентирующие деятельность по защите информации	**Знать:** Основные законы и подзаконные акты, документы Роскомнадзора в области информационной безопасности. **Уметь:** Верно трактовать и применять основные законы и подзаконные акты, документы Роскомнадзора в области информационной безопасности. **Владеть:** Навыками применения основных законов и подзаконных актов, документов Роскомнадзора в области информационной безопасности.
		ОПК-5.2 Применяет нормативные и методические документы, регламентирующие деятельность по защите информации	**Знать:** Основные нормативные и методические документы ФСТЭК в области информационной безопасности. **Уметь:** Грамотно использовать основные нормативные и методические документы ФСТЭК в области информационной безопасности. **Владеть:** Навыками применения основных нормативных и методических документов ФСТЭК в области информационной безопасности.
	ОПК-5.1 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	ОПК-5.1.1 Разрабатывает политику информационной безопасности открытых информационных систем	**Знать:** Знать содержание основных законов и подзаконных актов, нормативных и методических документов ФСТЭК, определяющих содержание политики информационной безопасности открытых информационных систем. **Уметь:** Грамотно выделить и обосновать структуру и содержание политики информационной безопасности для информационной системы конкретной организации. **Владеть:** Навыками разработки политик информационной безопасности (политики безопасности персональных данных) для конкретной организации определенного вида деятельности.
		ОПК-5.1.2 Реализует политику информационной безопасности открытых информационных систем	**Знать:** Знать содержание основных законов и подзаконных актов, нормативных и методических документов ФСТЭК, определяющих порядок реализации политики информационной безопасности в рамках конкретной организации. **Уметь:** Грамотно разработать алгоритм реализации политики безопасности в рамках конкретной организации. **Владеть:** Навыками организации контроля реализации политики информационной безопасности открытых информационных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1. Компетенция ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1.	Основы информационной безопасности
2.	Организационное и правовое обеспечение информационной безопасности
3.	Метрология, стандартизация и сертификация

2. Компетенция ОПК-5.1 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1.	Методы проектирования защищенных открытых информационных систем

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 зач. единиц, 180 часов.

Форма промежуточной аттестации: курсовая работа, экзамен.

Вид учебной работы	Всего часов	Семестр № 4
Общая трудоемкость дисциплины, час	180	180
Контактная работа (аудиторные занятия), в т.ч.:	90	90
лекции	34	34
лабораторные	17	17
практические	34	34
групповые консультации в период теоретического обучения и промежуточной аттестации	5	5
контроль самостоятельной работы	-	-
Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:	90	90
Курсовой проект	-	-
Курсовая работа	24	24
Расчетно-графическое задания	-	-
Индивидуальное домашнее задание	-	-
Самостоятельная работа на подготовку к аудиторным занятиям (лекции, практические занятия, лабораторные занятия)	30	30
Экзамен	36	36

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4.1 Наименование тем, их содержание и объем
Курс 5 Семестр 10

№ 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 дисциплину.				
	Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения. Содержание и задачи процесса управления ИБ АС и предприятия вцелом.	2	2	-	2
2.	Подходы к управлению ИБ.				
	Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии. Стандартизация в сфере управления ИБ. Ресурсы предприятия, подлежащие защите с точки зрения ИБ. Комплекс методов и средств защиты информации как объект управления ИБ.	6	6	-	2
3.	Назначение и содержание политики ИБ.				
	Назначение и содержание политики ИБ предприятия в целом, его структурных подразделений, частных политик безопасности. Средства их реализации.	4	8	-	4
4.	Субъекты процесса управления ИБ АС.				
	Состав, роль, место и особенности взаимодействия субъектов процесса управления ИБ АС. Планирование, мотивация и контроль выполнения персоналом требований документов по защите информации в организации.	6	6	-	4
5.	Аудит в области ИБ.				
	Назначение, цели и виды аудита ИБ АС. Требования к аудитору ИБ, особенности взаимодействия между аудитором и заказчиком. Оценка работы аудитора. Стандартизация в сфере аудита ИБ. Содержание и организация процесса аудита ИБ. Оценка рисков ИБ. Отчетные документы по результатам аудита. Выполнение рекомендаций по итогам проведения аудита ИБ.	10	8	3	4
6.	Создание системы защиты информации как элемент управления ИБ.				
	Выбор необходимых программных и программно-аппаратных средств защиты информации в АС, проектирование комплексной системы защиты информации предприятия эффективной с точки зрения решаемых задач и необходимых для этого ресурсов.	2	-	4	4
7.	Программные средства поддержки в сфере управления ИБ.				
	Программные средства автоматизации процедур проведения аудита ИБ и анализа политики ИБ. Программные средства поддержки процессов управления ИБ.	4	4	10	10
	ВСЕГО	34	34	17	30

4.2. Содержание практических (семинарских) занятий

№ п/п	Наименование раздела дисциплины	Тема практического занятия	К-во часов	К-во часов СРС
семестр № 10				
1	Введение в дисциплину	Концептуальная модель информационной безопасности организации. Построение подсистемы информационной безопасности	2	1
2	Подходы к управлению ИБ	Организационная структура системы обеспечения безопасности информации. Служба защиты информации (СЗИ). Функции, задача, ответственность, штатная структура СЗИ	6	3
3	Назначение и содержание политики ИБ	Глобальная и локальные политики управления защитой информации в информационно-телекоммуникационных системах.	8	4
4	Субъекты процесса управления ИБ АС	Международные и отечественные стандарты в области управления, оценки и аудиту информационной безопасности. Процессная модель управления информационной безопасностью.	6	3
5	Аудит в области ИБ	Методы оценки рисков информационной безопасности. Оценка информационных рисков с использованием методов системного анализа.	8	4
6	-	-	-	-
7	Программные средства поддержки в сфере управления ИБ.	Средства анализа защищенности информационно-телекоммуникационных систем. Выявление атак и управление информационными рисками.	4	2
		ИТОГО:	34	17
			ВСЕГО:	51

4.3. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	К-во часов СРС
семестр № 10				
5	Аудит в области ИБ	Использование инструментов оценки рисков и управления рисками информационной безопасности.	3	2
6	Создание системы защиты информации как элемент управления ИБ	Использование инструментальных средств для выявления уязвимостей и отражения атак	4	2
7	Программные средства поддержки в сфере управления ИБ.	Организация проведения экспертизы систем защиты информации в информационно-телекоммуникационных системах	10	4
		ИТОГО:	17	8
			ВСЕГО:	25

4.4. Содержание курсового проекта/работы

В качестве курсовой работы предлагается студентам выполнить построение системы защиты объекта информатизации организации (предприятия, органа государственной власти) по исходным данным.

Исходные данные обучаемые получают у преподавателя, и они включают

следующую информацию:

1. Государственная или негосударственная организация.
2. Отрасль деятельности организации.
3. Вид и структура объекта информатизации.
4. Количество автоматизированных рабочих мест.
5. Вид информации ограниченного доступа (персональные данные, служебная тайна, коммерческая или др. виды тайн).
6. Дополнительная информация.

В ходе выполнения курсовой работы необходимо выполнить следующие этапы:

1. Формирование требований к защите информации.
   - Обследование (аудит).
   - Выявление актуальных угроз.
   - Определение уровня защищенности (класса).
   - Определение требований к системе защиты информации.
2. Разработка и внедрение системы защиты информации.
   - Проектирование.
   - Разработка организационных мероприятий.
   - Реконфигурация информационной системы.
   - Подбор средств защиты информации.
   - Оценка соответствия системы защиты информации требованиям.

Объем курсовой работы должен составлять 12-15 листов печатного текста.

4.5. Содержание расчетно-графического задания, индивидуальных домашних заданий

Не предусмотрено учебным планом

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1. Реализация компетенций

1. Компетенция ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-5.1 Применяет нормативные правовые акты, регламентирующие деятельность по защите информации	устный опрос, защита курсовой и лабораторной работ, экзамен
ОПК-5.2 Применяет нормативные и методические документы, регламентирующие деятельность по защите информации	собеседование, защита курсовой и лабораторной работ, экзамен

2. Компетенция ОПК-5.1 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-5.1.1 Разрабатывает политику информационной безопасности открытых информационных систем	устный опрос, защита курсовой работы, экзамен
ОПК-5.1.2 Реализует политику информационной безопасности открытых информационных систем	устный опрос, защита курсовой работы, экзамен

5.2. Типовые контрольные задания для промежуточной аттестации

5.2.1. Перечень контрольных вопросов (типовых заданий) для экзамена

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1.	Введение в дисциплину	Основные определения в области управления ИБ Содержание и задачи процесса управления ИБ АС и предприятия в целом
2.	Подходы к управлению ИБ	Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии Ресурсы предприятия, подлежащие защите с точки зрения ИБ Комплекс методов и средств защиты информации как объект управления ИБ нормативно-методических и организационно-распорядительных документов по защите информации на предприятии Концепция безопасности предприятия и ИБ
3.	Назначение и содержание политики ИБ	Назначение и содержание политики ИБ предприятия в целом, его структурных подразделений, частных политик безопасности Модель нарушителя политики безопасности Типичные угрозы информации и уязвимости корпоративных АС Полномочия и ответственность персонала по защите информации на предприятии
4.	Субъекты процесса управления ИБ АС	Состав, роль, место и особенности взаимодействия субъектов процесса управления ИБ АС Организация контроля и мотивации выполнения персоналом требований нормативно-методических и организационно-распорядительных документов по защите информации на предприятии Организация контроля эффективности выполнения персоналом, ответственным за ИБ, своих функциональных обязанностей
5.	Аудит в области ИБ	Аудит информационной безопасности. Цели аудита Этапы (шаги аудита) информационной безопасности Основные стандарты в области управления ИБ и аудита ИБ. Их характеристика
6.	Создание системы защиты информации как элемент управления ИБ	Общая характеристика, состав стандарта OSI/ISO 27001-2005 Предпосылки проведения аудита ИБ Основные виды аудита ИБ Суть процессной модели управления ИБ Содержание стадий процессной модели «Планирование – Реализация – Проверка – Действие» Организация проведения работ по аудиту ИБ
7.	Программные средства поддержки в сфере управления ИБ	Выбор необходимых программных и программно-аппаратных средств защиты информации в АС Проектирование комплексной системы защиты информации предприятия эффективной с точки зрения решаемых задач и необходимых для этого ресурсов Программные средства автоматизации процедур проведения аудита ИБ и анализа политики ИБ Программные средства поддержки процессов управления ИБ

5.3. Типовые контрольные задания (материалы) для текущего контроля в семестре

Текущий контроль осуществляется в течение семестра в форме собеседования и устного опроса.

Собеседования и устные опросы направлены на проверку степени усвоения материала и понимания теоретических сведений, используемых в процессе выполнения работы. Примерные перечень вопросов для контроля знаний приведен в таблице:

Тематика дисциплины	Контрольные вопросы
Т.1. Введение в дисциплину	1. Дать понятие управлению ИБ 2. Система защиты информации в ИС 3. Задачи ИБ 4. Преимущества внедрения комплексной системы ИБ для структурных подразделений 5. Безопасность (защищенность) информации
Т.2. Подходы к управлению ИБ	1. Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии 2. Ресурсы предприятия, подлежащие защите с точки зрения ИБ 3. Комплекс методов и средств защиты информации как объект управления ИБ 4. нормативно-методических и организационно-распорядительных документов по защите информации на предприятии 5. Концепция безопасности предприятия и ИБ
Т.3. Назначение и содержание политики ИБ	1. Назначение и содержание политики ИБ предприятия в целом, его структурных подразделений, частных политик безопасности 2. Модель нарушителя политики безопасности 3. Типичные угрозы информации и уязвимости корпоративных АС 4. Полномочия и ответственность персонала по защите информации на предприятии
Т.4. Субъекты процесса управления ИБ АС	1. Состав, роль, место и особенности взаимодействия субъектов процесса управления ИБ АС 2. Организация контроля и мотивации выполнения персоналом требований нормативно-методических и организационно-распорядительных документов по защите информации на предприятии 3. Организация контроля эффективности выполнения персоналом, ответственным за ИБ, своих функциональных обязанностей
Т.5. Аудит в области ИБ	1. Аудит информационной безопасности. Цели аудита 2. Этапы (шаги аудита) информационной безопасности 3. Основные стандарты в области управления ИБ и аудита ИБ. Их характеристика
Т.6. Создание системы защиты информации как элемент управления ИБ	1. Общая характеристика, состав стандарта OSI/ISO 27001-2005 2. Предпосылки проведения аудита ИБ 3. Основные виды аудита ИБ 4. Суть процессной модели управления ИБ 5. Содержание стадий процессной модели «Планирование – Реализация – Проверка – Действие» 6. Организация проведения работ по аудиту ИБ
Т.7. Программные средства поддержки в сфере управления ИБ	1. Выбор необходимых программных и программно-аппаратных средств защиты информации в АС 2. Проектирование комплексной системы защиты информации предприятия эффективной с точки зрения решаемых задач и

	необходимых для этого ресурсов 3. Программные средства автоматизации процедур проведения аудита ИБ и анализа политики ИБ 4. Программные средства поддержки процессов управления ИБ

5.4. Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме экзамена используется следующая шкала оценивания: 2 – неудовлетворительно, 3 – удовлетворительно, 4 – хорошо, 5 – отлично.

Критериями оценивания достижений показателей являются:

Наименование показателя оценивания результата обучения по дисциплине	Критерий оценивания
Знания	Знание терминов, определений, понятий
	Знание основных закономерностей, соотношений, принципов
	Объем освоенного материала
	Полнота ответов на вопросы
	Четкость изложения и интерпретации знаний
Умения	Умение анализировать основные положения законодательства в области безопасности информации
	Умение использовать руководящие документы регуляторов в области информационной безопасности
Навыки	Владение навыками теоретического и экспериментального исследования объектов профессиональной деятельности
	Качество выполнения исследований объектов профессиональной деятельности
	Самостоятельность выполнения исследований объектов профессиональной деятельности

Оценка преподавателем выставляется интегрально с учётом всех показателей и критериев оценивания.

Оценка сформированности компетенций по показателю Знания.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Знание терминов, определений, понятий	Не знает терминов и определений	Знает термины и определения, но допускает неточности формулировок	Знает термины и определения	Знает термины и определения, может корректно сформулировать их самостоятельно
Знание основных закономерностей, соотношений, принципов	Не знает основные закономерности и соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний, их интерпретирует и использует	Знает основные закономерности, соотношения, принципы построения знаний, может самостоятельно их получить и использовать
Объем освоенного материала	Не знает значительной части материала дисциплины	Знает только основной материал дисциплины, не	Знает материал дисциплины в достаточном объеме	Обладает твердым и полным знанием материала дисциплины,

		усвоил его деталей		владеет дополнительными знаниями
Полнота ответов на вопросы	Не дает ответы на большинство вопросов	Дает неполные ответы на все вопросы	Дает ответы на вопросы, но не все - полные	Дает полные, развернутые ответы на поставленные вопросы
Четкость изложения и интерпретации знаний	Излагает знания без логической последовательности	Излагает знания с нарушениями в логической последовательности	Излагает знания без нарушений в логической последовательности	Излагает знания в логической последовательности, самостоятельно их интерпретируя и анализируя
	Не иллюстрирует изложение поясняющими схемами, рисунками и примерами	Выполняет поясняющие схемы и рисунки небрежно и с ошибками	Выполняет поясняющие рисунки и схемы корректно и понятно	Выполняет поясняющие рисунки и схемы точно и аккуратно, раскрывая полноту усвоенных знаний
	Неверно излагает и интерпретирует знания	Допускает неточности в изложении и интерпретации знаний	Грамотно и по существу излагает знания	Грамотно и точно излагает знания, делает самостоятельные выводы

Оценка сформированности компетенций по показателю Умения.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Умение применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Не умеет применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Допускает неточности при применении нормативные правовые актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Умеет применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Умеет применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации и делать обобщающие выводы
Умение разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	Не умеет разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	Разработка и реализация политики информационной безопасности открытых информационных систем вызывает затруднения	Осуществляет разработку и реализует политику информационной безопасности открытых информационных систем	Умело осуществляет разработку и реализует политику информационной безопасности открытых информационных систем для решения типовых задач

Оценка сформированности компетенций по показателю Навыки.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Владение навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Не владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Не достаточно хорошо владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Профессионально владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности
Качество выполнения исследований объектов профессиональной деятельности	Не качественно выполняет исследования объектов профессиональной деятельности, допускает грубые ошибки	Не достаточно качественно выполняет исследования объектов профессиональной деятельности, допускает и исправляет ошибки с посторонней помощью	Не достаточно качественно выполняет исследования объектов профессиональной деятельности, допускает и исправляет ошибки самостоятельно	Качественно выполняет исследования объектов профессиональной деятельности
Самостоятельность выполнения исследований объектов профессиональной деятельности	Не может самостоятельно выполнять исследования объектов профессиональной деятельности	Выполняет исследования объектов профессиональной деятельности с посторонней помощью	При выполнении исследования объектов профессиональной деятельности иногда требуется посторонняя помощь	Самостоятельно выполняет исследования объектов профессиональной деятельности

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

6.1. Материально-техническое обеспечение

№	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1.	Учебная аудитория для проведения лекционных занятий	Специализированная мебель. Мультимедийная установка, экран, доски
2.	Учебная аудитория для проведения практических занятий	Специализированная мебель. Компьютеры на базе процессоров Intel или AMD.
3.	Читальный зал библиотеки для самостоятельной работы	Специализированная мебель. Компьютерная техника, подключенная к сети интернет и имеющая доступ в электронно-образовательную среду.

6.2. Лицензионное и свободно распространяемое программное обеспечение

№	Перечень лицензионного программного обеспечения.	Реквизиты подтверждающего документа
1	Microsoft Windows 10 Корпоративная	(Соглашение Microsoft Open Value Subscription V9221014 Соглашение действительно с 01.11.2020 по 31.10.2023). Договор поставки ПО № 128-21 от 30.10.2021.
2	Microsoft Office Professional Plus 2016	(Соглашение Microsoft Open Value Subscription V9221014 Соглашение действительно с 01.11.2020 по 31.10.2023). Договор поставки ПО № 128-21 от 30.10.2021.
3	Kaspersky Endpoint Security «Стандартный Russian Edition»	Сублицензионный договор № 102 от 24.05.2018. Срок действия лицензии до 19.08.2020 Гражданско-правовой Договор (Контракт) № 27782 «Поставка продления права пользования (лицензии) Kaspersky Endpoint Security от 03.06.2020. Срок действия лицензии 19.08.2022г.
4	Среды программирования Free Pascal, Dev C++ или CodeBlocks	Свободно распространяемое ПО согласно условиям лицензионного соглашения

6.3. Перечень учебных изданий и учебно-методических материалов

Перечень основной литературы

1. Анисимов А. А. Менеджмент в сфере информационной безопасности/А. А. Анисимов. – 2012. – 176 с., ISBN 978-5-9963-0237-6 (3 экз)
2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – 2-е изд. исп. и доп. – М.: Горячая линия – Телеком, 2013. – 338 с.
3. Малюк А.А. Теория защиты информации [Электронный ресурс]: монография/ Малюк А.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/12048.— ЭБС «IPRbooks»
4. Милославская Н.Г. Технические, организационные и кадровые аспекты управления информационной безопасностью [Электронный ресурс]: учебное пособие/ Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 214 с.— Режим доступа: http://www.iprbookshop.ru/12056.— ЭБС «IPRbooks».
5. 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».
6. Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2006. — 264 с. — ISBN 5-9556-0053-1. (14 экз)
7. Фороузан Бехроуз А. Криптография и безопасность сетей [Электронный ресурс]: учебное пособие/ Фороузан Бехроуз А.— Электрон. текстовые данные.— М.: БИНОМ. Лаборатория знаний, Интернет-Университет Информационных Технологий (ИНТУИТ), 2010.— 784 с.— Режим доступа: http://www.iprbookshop.ru/15847.— ЭБС «IPRbooks».
8. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. / В.Ф. Шаньгин, Москва, ДМК Пресс, 2012. - 592 с.: ил.
9. Галатенко В.А. Основы информационной безопасности : курс лекций : учеб. пособие / В. А. Галатенко. - 3-е изд. - Москва : Интернет-Университет Информационных Технологий, 2006. - 205 с. - (Основы информационных технологий). (1 экз)
10. Гончаренко Л.П. Управление безопасностью : учеб. пособие / Л. П. Гончаренко, Е. С. Куценко. - Москва : КноРус, 2005. - 272 с. (7 экз)

Перечень дополнительной и справочной литературы

1. Федеральный закон от 27.07.06 г. № 149 – ФЗ «Об информации, информационных технологиях и защите информации».
2. Федеральный закон от 27.07.06 г. № 152 – ФЗ «О персональных данных».
3. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».
4. Международный стандарт ISO/IEC 27002-2005 «Информационные технологии. Свод правил по управлению защитой информации».

5. ГОСТ Р ИСО/МЭК 15408-1-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».
6. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».
7. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий».
8. ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
9. ГОСТ 34.201 - 89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.
10. ГОСТ 34.601 - 90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
11. ГОСТ 34.602 - 89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

6.4. Перечень интернет ресурсов, профессиональных баз данных, информационно-справочных систем

1. Электронная библиотека (на базе ЭБС «БиблиоТех») — Режим доступа: http://ntb.bstu.ru
2. Электронно-библиотечная система IPRbooks — Режим доступа: http://www.iprbookshop.ru
3. Электронно-библиотечная система «Университетская библиотека ONLINE» — Режим доступа: http://www.biblioclub.ru/

7. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа утверждена на 202__/202__ учебный год без изменений / с изменениями, дополнениями

Протокол № _____ заседания кафедры от «____»_____ 202_ г.

Заведующий кафедрой_____
подпись, ФИО

Директор института _____
подпись, ФИО