

**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.

2021 г.

**РАБОЧАЯ ПРОГРАММА**  
дисциплины

**Организационное и правовое обеспечение информационной безопасности**

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
Обще-профессиональные 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	<p><b>Знать:</b> основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации;</p> <p><b>Уметь:</b> разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации;</p> <p><b>Владеть:</b> навыками работы с нормативными правовыми актами</p>
		ОПК-5.2 Применяет нормативные и методические документы, регламентирующие деятельность по защите информации	<p><b>Знать:</b> терминологию, основные руководящие и регламентирующие документы в области защиты информации;</p> <p><b>Уметь:</b> применять действующую законодательную базу в области обеспечения информационной безопасности;</p> <p><b>Владеть:</b> навыками работы с нормативными правовыми актами</p>
	ОПК-6 Способен при решении профессиональных задач организовать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами,	ОПК-6.1 Решает профессиональные задачи по защите информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами	<p><b>Знать:</b> правовые нормы и стандарты по лицензированию в области обеспечения защиты конфиденциальной информации и сертификации средств защиты информации;</p> <p><b>Уметь:</b> применять действующую нормативно-правовую базу в области обеспечения информационной безопасности;</p> <p><b>Владеть:</b> навыками работы с нормативными правовыми актами</p>

	<p>нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p>	<p>ОПК-6.2 Решает профессиональные задачи по защите информации ограниченного доступа в автоматизированных системах в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p>	<p><b>Знать:</b> содержание основных нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; <b>Уметь:</b> применять действующую нормативную базу ФСБ и ФСТЭК для построения системы защиты информации; <b>Владеть:</b> навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации.</p>
--	---	--	---

## 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.	Метрология, стандартизация и сертификация
3.	Организационное и правовое обеспечение информационной безопасности.
4.	Управление информационной безопасностью.

**2. Компетенция ОПК-6.** Способен при решении профессиональных задач организовать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1.	Защита информации от утечки по техническим каналам
2.	Организационное и правовое обеспечение информационной безопасности.

### 3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зач. единиц, 144 часов.

Форма промежуточной аттестации: экзамен.

Вид учебной работы	Всего часов	Семестр № 6
Общая трудоемкость дисциплины, час	144	144
<b>Контактная работа (аудиторные занятия), в т.ч.:</b>	73	73
лекции	34	34
лабораторные	-	-
практические	34	34
групповые консультации в период теоретического обучения и промежуточной аттестации	5	5
контроль самостоятельной работы	-	-
<b>Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:</b>	71	71
Курсовой проект	-	-
Курсовая работа	-	-
Расчетно-графическое задания	-	-
Индивидуальное домашнее задание	-	-
Самостоятельная работа на подготовку к аудиторным занятиям (лекции, практические занятия, лабораторные занятия)	35	35
Экзамен	36	36

**4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ**  
**4.1 Наименование тем, их содержание и объем**  
**Курс 5 Семестр 9**

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
<b>1. Предмет, методология и понятийный аппарат курса.</b>					
	Цель и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия. Порядок изучения дисциплины. Определение понятия информации. Классификация информации. Источники и методы сбора информации. Получение информации из различных источников.	4	4	-	4
<b>2. Обеспечение безопасности информации и компетенция органов власти по обеспечению информационной безопасности.</b>					
	Понятия информационная и компьютерная безопасность. Содержание понятия информационная безопасность (ИБ). Основные проблемы ИБ. Задачи государственной системы ИБ. Направление деятельности по обеспечению ИБ в организациях. Компетенции органов власти в сфере ИБ: ФСБ России, СВР России, ФСО, ФСТЭК.	4	4	-	4
<b>3. Правовые основы обеспечения информационной безопасности.</b>					
	Конституция РФ. Концептуальные документы о сфере ИБ: Доктрина информационной безопасности РФ. Концепция использования информационных технологий. Гражданский кодекс РФ.	6	4	-	5
<b>4. Федеральные и ведомственные нормативные акты в области ИБ.</b>					
	Федеральные законы: «О государственной тайне», «О коммерческой тайне», «О лицензировании отдельных видов деятельности», «О техническом регулировании», «О персональных данных», «Об электронной подписи», «Об информации, информационных технологиях и защите информации», «О лицензировании отдельных видов деятельности». Основные подзаконные акты: Указы Президента РФ, Постановления Правительства РФ. Правонарушения и преступления в сфере ИТ.	4	6	-	6
<b>5. Международные и отечественные стандарты в сфере ИБ.</b>					
	Исторический очерк развития зарубежных стандартов в сфере ИБ. Критерии безопасности компьютерных систем США: «Оранжевая книга». Европейские критерии безопасности ИТ. Федеральные критерии безопасности ИТ. Канадские критерии безопасности компьютерных систем. Общие критерии безопасности ИТ. Система государственных и отраслевых стандартов	4	4	-	4

	России в сфере ИБ. ГОСТы Р ИСО/МЭК: 15408-2002, 17799-2005, 27001-2006, нормативные документы ФСТЭК.				
6. Лицензирование, сертификация и аттестация в сфере ИБ.					
	Лицензирование деятельности в сфере ИБ. Сертификация продукции в сфере ИБ. Добровольная сертификация. Обязательное подтверждение соответствия. Порядок проведения сертификационных испытаний. Аттестация объектов информатизации. Сертификация на международном и региональном уровнях. Сертификация продукции, ввозимой из-за границы.	6	6	-	6
7. Организационное обеспечение ИБ.					
	Концепция безопасности организации и ее содержание. Политика информационной безопасности. Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников. Варианты организационных структур, обеспечивающих защиту информации. Функции их структурных единиц. Основные документы службы информационной безопасности: план работы, задания на поиск информации, отчеты о выполненных работах.	6	6	-	6
	ВСЕГО	34	34	-	35

#### 4.2. Содержание практических (семинарских) занятий

№ п/п	Наименование раздела дисциплины	Тема практического занятия	К-во часов	К-во часов СРС
семестр № 9				
1.	Предмет, методология и понятийный аппарат курса	Классификация информации. Источники и методы сбора информации.	4	3
2.	Обеспечение безопасности информации и компетенция органов власти по обеспечению информационной безопасности	Направление деятельности по обеспечению ИБ в организациях. Компетенции органов власти в сфере ИБ: ФСБ России, СВР России, ФСО, ФСТЭК	4	3
3.	Правовые основы обеспечения информационной безопасности	Концепция использования информационных технологий. Гражданский кодекс РФ	4	3
4.	Федеральные и ведомственные нормативные акты в области ИБ	Основные подзаконные акты: Указы Президента РФ, Постановления Правительства РФ. Правонарушения и преступления в сфере ИТ	6	5
5.	Международные и отечественные стандарты в сфере ИБ	Основные подзаконные акты: Указы Президента РФ, Постановления Правительства РФ. Правонарушения и преступления в сфере ИТ	4	3
6.	Лицензирование, сертификация и аттестация в сфере ИБ	Порядок проведения сертификационных испытаний. Аттестация объектов информатизации. Сертификация на международном и региональном уровнях.	6	5



		Сертификация продукции, ввозимой из-за границы.		
7.	Организационное обеспечение ИБ	Варианты организационных структур, обеспечивающих защиту информации. Функции их структурных единиц. Основные документы службы информационной безопасности: план работы, задания на поиск информации, отчеты о выполненных работах	6	5
ИТОГО:			34	27
ВСЕГО:				61

#### **4.3. Содержание лабораторных занятий**

Не предусмотрено учебным планом

#### **4.4. Содержание курсового проекта/работы**

Не предусмотрено учебным планом

#### **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-10.1 Анализирует криптографические методы, реализованные в средствах защиты информации	устный опрос, экзамен
ОПК-10.2 Использует средства криптографической защиты информации при решении задач профессиональной деятельности	собеседование на практическом занятии, экзамен

**2. Компетенция ОПК-6. Способен при решении профессиональных задач организовать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю**

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-10.1 Анализирует криптографические методы, реализованные в средствах защиты информации	устный опрос, экзамен
ОПК-10.2 Использует средства криптографической защиты информации при решении задач профессиональной деятельности	Собеседование на практическом занятии, 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.	Предмет, методология и понятийный аппарат курса	Место информационной безопасности экономических систем в национальной безопасности страны. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
2.	Обеспечение безопасности информации и компетенция органов власти по обеспечению	Каковы современные проблемы защиты служебной тайны? Что такое банковская тайна и в чем заключается специфика ее защиты? Анализ способов нарушений информационной безопасности. Виды противников или "нарушителей". Источники и мотивы нарушений. Преднамеренные действия сотрудников. Анализ способов нарушений информационной безопасности. Виды противников или "нарушителей". Источники и мотивы нарушений. Действия сторонних лиц

	информационн ой безопасности	криминального характера. Основные технологии построения защищенных ЭИС. Контроль жизненного цикла программного обеспечения с точки зрения информационной безопасности. Мероприятия, осуществляемые при создании ИС. Сертификация программного обеспечения. Основные технологии построения защищенных ЭИС. Контроль жизненного цикла программного обеспечения с точки зрения информационной безопасности. Мероприятия, осуществляемые в процессе эксплуатации ИС.
3.	Правовые основы обеспечения информационн ой безопасности	Законодательный уровень защиты информации. Основные положения Конституции РФ о защите информации, правах граждан на получение и распространение информации, законы и законодательные акты Российской Федерации в области защиты информации. Основные положения теории информационной безопасности информационных систем. Конфиденциальность. Целостность. Доступность. Объект и субъект доступа. Средство работы с информацией. Несанкционированный доступ к информации. Идентификация. Аутентификация. Принципы распределения прав и ответственности.
4.	Федеральные и ведомственные нормативные акты в области ИБ	Основные положения закона «Об информации, информатизации и защите информации», определение понятий информации, документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов. Закон "О лицензировании отдельных видов деятельности. Определение понятий лицензии, лицензируемого вида деятельности, лицензирования, лицензирующие органов, лицензиата. Положение статьи 17 Закона о видах деятельности, на осуществление которых требуются лицензии. Основные положения закона РФ «Об электронной подписи» об электронном документе и электронной подписи, сертификате ЭП, владельце ЭП, закрытом и открытом ключе ЭП. Правовой режим обеспечения безопасности персональных данных. Особенности обработки персональных данных осуществляемой без использования средств автоматизации. Особенности обеспечения безопасности персональных данных операторами, являющимися государственными либо муниципальными органами. Особенности обработки биометрических персональных данных. Правовой режим обеспечения безопасности государственных и муниципальных систем. Режим защиты коммерческой тайны. Особенности института коммерческой тайны. Механизм защиты коммерческой тайны. Перечислите субъекты и объекты правоотношений в сфере защиты государственной тайны. Раскройте принципы раскредивания. Особенности механизма засекречивания. Дайте сравнительный анализ механизмов засекречивания в России и США. Реквизиты носителей государственной тайны. В чем заключаются особенности раскредивания? Система органов защиты государственной тайны, основные полномочия включенных в нее органов государственной власти. Перечислите основные правовые механизмы допуска граждан к государственной тайне. В чем заключается и из чего состоит механизм распоряжения государственной тайной? Перечислите признаки состава преступления и раскройте их понятие. Каковы составы преступления, являющихся нарушением тайны сообщений и отказом в информации? Уголовно-правовая защита конфиденциальной информации.
5.	Международны е и	Международные стандарты информационного обмена. «Оранжевая книга» США как критерий классификации систем информационной

	отечественные стандарты в сфере ИБ	безопасности. «Общие критерии» стран Европейского сообщества, их основные положения. Системы управления (менеджмента) информационной безопасности. Принципы построения. Планирование системы управления (менеджмента) информационной безопасности. Внедрение системы управления (менеджмента) информационной безопасности. Мониторинг и анализ и Сопровождение и совершенствование системы управления (менеджмента) информационной безопасности.
6.	Лицензирование, сертификация и аттестация в сфере ИБ	Лицензирования и сертификации в области технической защите конфиденциальной информации. Система сертификации средств защиты информации требованиям безопасности информации. Правовая основа функционирования систем лицензирования и сертификации в области защиты информации. Перечислите уполномоченные органы лицензирования и их основные обязанности. В чем заключаются особенности проведения специальных экспертиз? Каковы особенности сертификации средств защиты информации? Раскройте структуру государственной системы сертификации и полномочия центральных и федеральных органов. В чем заключаются испытания средств защиты информации? Опишите систему государственной аттестации руководителей и специалистов в области защиты информации.
7.	Организационное обеспечение ИБ	Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа. Оценка соответствия объектов информатизации требованиям безопасности информации. Классификация автоматизированных систем и требования по защите информации. Дайте характеристику неправомерного доступа к компьютерной информации как уголовного преступления. Каковы составы преступлений в части создания, использования и распространения вредоносных программ для ЭВМ? В чем заключается нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, как уголовного преступления?

### 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
Предмет, методология и понятийный аппарат курса	<ol style="list-style-type: none"> <li>1. Место информационной безопасности экономических систем в национальной безопасности страны.</li> <li>2. Информационная безопасность в условиях функционирования в России глобальных сетей.</li> <li>3. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.</li> <li>4. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.</li> </ol>
Обеспечение безопасности информации и компетенция органов	<ol style="list-style-type: none"> <li>1. Каковы современные проблемы защиты служебной тайны?</li> <li>2. Что такое банковская тайна и в чем заключается специфика ее защиты?</li> <li>3. Анализ способов нарушений информационной безопасности.</li> </ol>

<p>власти по обеспечению информационной безопасности</p>	<ol style="list-style-type: none"> <li>4. Виды противников или «нарушителей».</li> <li>5. Источники и мотивы нарушений.</li> <li>6. Преднамеренные действия сотрудников. Анализ способов нарушений информационной безопасности.</li> <li>7. Виды противников или «нарушителей». Источники и мотивы нарушений.</li> <li>8. Действия сторонних лиц криминального характера.</li> <li>9. Основные технологии построения защищенных ЭИС.</li> <li>10. Контроль жизненного цикла программного обеспечения с точки зрения информационной безопасности.</li> <li>11. Мероприятия, осуществляемые при создании ИС.</li> <li>12. Основные технологии построения защищенных ЭИС.</li> <li>13. Контроль жизненного цикла программного обеспечения с точки зрения информационной безопасности.</li> <li>14. Мероприятия, осуществляемые в процессе эксплуатации ИС.</li> </ol>
<p>Правовые основы обеспечения информационной безопасности</p>	<ol style="list-style-type: none"> <li>1. Законодательный уровень защиты информации.</li> <li>2. Основные положения Конституции РФ о защите информации, правах граждан на получение и распространение информации, законы и законодательные акты Российской Федерации в области защиты информации.</li> <li>3. Основные положения теории информационной безопасности информационных систем. Конфиденциальность. Целостность. Доступность. Объект и субъект доступа.</li> <li>4. Средство работы с информацией.</li> <li>5. Несанкционированный доступ к информации.</li> <li>6. Идентификация. Аутентификация.</li> <li>7. Принципы распределения прав и ответственности.</li> </ol>
<p>Федеральные и ведомственные нормативные акты в области ИБ</p>	<ol style="list-style-type: none"> <li>1. Основные положения закона «Об информации, информатизации и защите информации», определение понятий информации, документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов.</li> <li>2. Закон "О лицензировании отдельных видов деятельности.</li> <li>3. Определение понятий лицензии, лицензируемого вида деятельности, лицензирования, лицензирующие органов, лицензиата.</li> <li>4. Положение статьи 17 Закона о видах деятельности, на осуществление которых требуются лицензии.</li> <li>5. Основные положения закона РФ «Об электронной подписи» об электронном документе и электронной подписи, сертификате ЭП, владельце ЭП, закрытом и открытом ключе ЭП.</li> <li>6. Правовой режим обеспечения безопасности персональных данных.</li> <li>7. Особенности обработки персональных данных осуществляемой без использования средств автоматизации.</li> <li>8. Особенности обеспечения безопасности персональных данных операторами, являющимися государственными либо муниципальными органами.</li> <li>9. Особенности обработки биометрических персональных данных.</li> <li>10. Правовой режим обеспечения безопасности государственных и муниципальных систем.</li> <li>11. Режим защиты коммерческой тайны. Особенности института коммерческой тайны. Механизм защиты коммерческой тайны.</li> <li>12. Перечислите субъекты и объекты правоотношений в сфере защиты государственной тайны.</li> <li>13. Раскройте принципы рассекречивания.</li> </ol>

	<p>14. Особенности механизма засекречивания. Дайте сравнительный анализ механизмов засекречивания в России и США.</p> <p>15. Реквизиты носителей государственной тайны. В чем заключаются особенности рассекречивания?</p> <p>16. Система органов защиты государственной тайны, основные полномочия включенных в нее органов государственной власти.</p> <p>17. Перечислите основные правовые механизмы допуска граждан к государственной тайне.</p> <p>18. Перечислите признаки состава преступления и раскройте их понятие.</p> <p>19. Каковы составы преступления, являющихся нарушением тайны сообщений и отказом в информации?</p> <p>20. Уголовно-правовая защита конфиденциальной информации.</p>
<p>Международные и отечественные стандарты в сфере ИБ</p>	<p>1. Международные стандарты информационного обмена. «Оранжевая книга» США как критерий классификации систем информационной безопасности. «Общие критерии» стран Европейского сообщества, их основные положения.</p> <p>2. Системы управления (менеджмента) информационной безопасности. Принципы построения.</p> <p>3. Планирование системы управления (менеджмента) информационной безопасности.</p> <p>4. Внедрение системы управления (менеджмента) информационной безопасности.</p> <p>5. Мониторинг, анализ, сопровождение и совершенствование системы управления (менеджмента) информационной безопасности.</p>
<p>Лицензирование, сертификация и аттестация в сфере ИБ</p>	<p>1. Лицензирования и сертификации в области технической защите конфиденциальной информации.</p> <p>2. Система сертификации средств защиты информации требованиям безопасности информации.</p> <p>3. Правовая основа функционирования систем лицензирования и сертификации в области защиты информации.</p> <p>4. Перечислите уполномоченные органы лицензирования и их основные обязанности.</p> <p>5. В чем заключаются особенности проведения специальных экспертиз?</p> <p>6. Каковы особенности сертификации средств защиты информации?</p> <p>7. Раскройте структуру государственной системы сертификации и полномочия центральных и федеральных органов.</p> <p>8. В чем заключаются испытания средств защиты информации? Опишите систему государственной аттестации руководителей и специалистов в области защиты информации.</p> <p>9. Сертификация программного обеспечения.</p>
<p>Организационное обеспечение ИБ</p>	<p>1. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа.</p> <p>2. Оценка соответствия объектов информатизации требованиям безопасности информации.</p> <p>3. Классификация автоматизированных систем и требования по защите информации.</p> <p>4. Дайте характеристику неправомерного доступа к компьютерной информации как уголовного преступления.</p> <p>5. Каковы составы преступлений в части создания, использования и распространения вредоносных программ для ЭВМ?</p> <p>6. В чем заключается нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, как уголовного преступления?</p>

#### 5.4. Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме зачета 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 усвоил его	Знает материал дисциплины в достаточном объеме	Обладает твердым и полным знанием материала дисциплины, владеет

		деталей		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 анализировать содержание основных законодательных актов и руководящих документов ФСБ и ФСТЭК	Не умеет анализировать содержание основных законодательных актов и руководящих документов ФСБ и ФСТЭК	Допускает неточности в анализе содержания основных законодательных актов и руководящих документов ФСБ и ФСТЭК	Умеет анализировать содержание основных законодательных актов и руководящих документов ФСБ и ФСТЭК	Умеет анализировать содержание основных законодательных актов и руководящих документов ФСБ и ФСТЭК и делать обобщающие выводы
Умение использовать нормативные документы регуляторов для обеспечения организационной защиты информации	Не умеет использовать нормативные документы регуляторов для обеспечения организационной защиты информации	Использование нормативных документов регуляторов для обеспечения организационной защиты информации вызывает затруднения	Умеет использовать нормативные документы регуляторов для обеспечения организационной защиты информации	Умело использует нормативные документы регуляторов для обеспечения организационной защиты информации

### Оценка сформированности компетенций по показателю Навыки.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Владение навыками теоретического и	Не владеет навыками теоретического и	Не достаточно хорошо владеет навыками	Владеет навыками теоретического	Профессионально владеет навыками теоретического и



экспериментального исследования объектов профессиональной деятельности	экспериментального исследования объектов профессиональной деятельности	теоретического и экспериментального исследования объектов профессиональной деятельности	и экспериментального исследования объектов профессиональной деятельности	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

1. Башлы П.Н. Информационная безопасность: учебно-практическое пособие / Башлы П.Н., Бабаш А.В., Баранова Е.К. - М.: Изд. центр ЕАОИ, 2011. - 376 с. <http://www.biblioclub.ru/book/90539/>

2. 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>.— ЭБС «IPRbooks»

3. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности. [Электронный ресурс] : Учебные пособия / Н.С. Кармановский, О.В. Михайличенко, С.В. Савков. — Электрон. дан. — СПб. : НИУ ИТМО, 2013. — 148 с. — Режим доступа: <http://e.lanbook.com/book/43579>

4. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности. [Электронный ресурс] : Учебные пособия — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 140 с. — Режим доступа: <http://e.lanbook.com/book/5163>

5. Креопалов В. В. Технические средства и методы защиты информации: учебно-практическое пособие / В.В. Креопалов. - М.: Изд. центр ЕАОИ, 2011.- 278 с. <http://www.biblioclub.ru/book/90753/>

6. Куняев Н.Н. Правовое обеспечение национальных интересов Российской Федерации и информационной сфере / Н.Н. Куняев. — М.: Логос, 2010. - 348 с. <http://www.biblioclub.ru/book/84990/>

7. Ярочкин В.И. Информационная безопасность [Электронный ресурс]: учебник для вузов/ Ярочкин В.И.— Электрон. текстовые данные.— М.: Академический Проект, 2008.— 544 с.— Режим доступа: <http://www.iprbookshop.ru/36331.html>.— ЭБС «IPRbooks»

8. Алешенков М. Основы национальной безопасности/М.Алешенков /Основы безопасности жизни.-2005.-№11.-С.5-10. [текст]

9. Брандман Э. М. Глобализация и информационная безопасность общества/Э.М.Брандман //Философия и общество.-2006.-№1.-С.31-41. [текст]

10. Брандман Э. М. Цивилизационные императивы и приоритеты информационной безопасности общества/Э.М.Брандман //Философия и общество.-2006.-№3.-С.60-77.-Предпринимательство, с.131-144. [текст]

11. Доктрина информационной безопасности //Средства массовой информации постсоветской России: Учеб. пособие /Я.Н. Засурский, Е. Л. Вартанова, И.И. Засурский.-М., 2002.-С.262-301. [текст]

12. Егозина В. Смотреть нельзя запретить (агрессивная информационная среда как угроза для безопасности)/В. Егозина, Н. Овчинников //ОБЖ.- 2003.-№4.-С.15-18. [текст]

13. Еляков А.Д. Информационная свобода человека/А.Д.Еляков // Социально-гуманитарные знания.-2005.-№3.-С.125-141. [текст]

14. Жигулин, Г.П. Организационное и правовое обеспечение информационной безопасности. [Электронный ресурс] : Учебные пособия — Электрон. дан. — СПб. : НИУ ИТМО, 2014. — 173 с. — Режим доступа:

<http://e.lanbook.com/book/70952>

15. Кожуханов, Н.М. Правовые основы информационной безопасности: учебное пособие. [Электронный ресурс] : Учебные пособия / Н.М. Кожуханов, Е.С. Недосекова. — Электрон. дан. — М. : РТА, 2013. — 88 с. — Режим доступа: <http://e.lanbook.com/book/74237>

16. Мамаев С.М., Петренко. Технологии защиты информации в Интернете. Санкт-Петербург, Изд-во «ПИТЕР». Москва-Харьков-Минск. 2002г.[текст]

17. Морозов И. Л. Информационная безопасность политической системы / И.Л.Морозов //ПОЛИС.-2002.-№5.-С.134-146. [текст]

18. Норткат С., Новак Д.- Обнаружение нарушений безопасности в сетях. Изд-й дом Вильямс, 2003г. [текст]

19. Поляков В. П. Практическое занятие по изучению вопросов информационной безопасности/В.П.Поляков //Информатика и образование.-2006.-№11.-С.75-80. [текст]

20. Поляков В.П. Информационная безопасность в курсе информатики /В.П.Поляков //Информатика и образование.-2006.-№10.-С.116-119.[текст]

#### Нормативные документы

1. Всеобщая декларация прав человека (от 10 декабря 1948 г.). М., 2010.
2. Конституция РФ. М., 2010.
3. Гражданский кодекс РФ. М., 2010.
4. Доктрина информационной безопасности РФ. М., 2010.
5. Федеральный закон «О государственной тайне» от 21 июля 1993 г. № 5485-1. М., 1993.
6. Федеральный закон «Об авторском праве и смежных правах» от 9 июля 1993 г. № 5351-1 (с последующими изменениями). М., 1993.
7. Федеральный закон «Об электронной цифровой подписи» от 10 января 2002 г. № 1-ФЗ. М., 2002.
8. Закон Российской Федерации от 21.07.1993г. № 5485-1 «О государственной тайне». // Российская газета от 21.09.1992г.
9. Федеральный закон РФ от 10.01.2002г. № 1-ФЗ «Об электронной цифровой подписи» // Российская газета, 12.01.2002.
10. ГОСТ РВ 51987-02 «Типовые требования и показатели качества функционирования информационных систем».
11. ГОСТ Р ИСО/МЭК 15408-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
12. ГОСТ Р ИСО/МЭК 27001-2006. «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента в информационной безопасности. Требования». М.: ИПК Издательство стандартов, 2007.

#### **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/>
  4. <http://www.consultantplus.ru/> - нормативно-правовая база
  5. <http://www.garant.ru/> - нормативно-правовая база
  6. <http://www.promo.s-director.ru/> – сайт журнала «Директор по безопасности»
  7. <http://college.ru/UDP/texts/> – учебный курс «Защита информации»;
  8. <http://www.mirash.ru/doki11.html> - нормативная база по защите информации;
  9. <http://tk.plexor.ru/web-links/info/38-zakon.html> - нормативные документы по защите информации.
  10. <http://www.inattack.ru/> - антивирусное программное обеспечение
  11. <http://securityvulns.ru/> - нормативные документы по защите информации
  12. [http://www.glossary.ru/cgi-bin/gl\\_sch2.cgi?RIt\(uwsg.outtg9!hlnuvngxтуху](http://www.glossary.ru/cgi-bin/gl_sch2.cgi?RIt(uwsg.outtg9!hlnuvngxтуху)
  13. <http://www.gosecure.ru/> - сайт форматов ЭЦП
  14. <http://z-oleg.com/> - антивирусное программное обеспечение
  15. <http://www.aladdin.ru/> - сайт производителя средств защиты информации