МИНОБРНАУКИ РОССИИ
Глазовский инженерно-экономический институт (филиал)
Федерального государственного бюджетного образовательного
учреждения высшего образования
«Ижевский государственный технический университет
имени М.Т. Калашникова»
(ГИЭИ (филиал) ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)

Бабушкин
Михаил
Анатольевич

УТВЕРЖДАЮ
Директор
_____/Бабушкин М.А.
_____ 2021г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

_____Правовые основы информационной безопасности _____
наименование – полностью

направление (специальность)
_____09.03.01 Информатика и вычислительная техника_____
код, наименование – полностью

направленность (профиль/
программа/специализация) ___ Автоматизированные системы обработки информации и управления _____
наименование – полностью

уровень образования: бакалавриат_____
удалить ненужные варианты

форма обучения: _____очная_____
очная/очно-заочная/заочная

общая трудоемкость дисциплины составляет: ____3_____ зачетных единиц(ы)

Кафедра ___Машиностроение и информационные технологии_____
полное наименование кафедры, представляющей рабочую программу

Составитель _____Горбушин А.Г. к.п.н., доцент _____
Ф.И.О.(полностью), степень, звание

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования и рассмотрена на заседании кафедры

Протокол от 21.05.2021 г. № 5

Заведующий кафедрой _____А.Г. Горбушин

21.05 2021 г.

СОГЛАСОВАНО

Количество часов рабочей программы и формируемые компетенции соответствуют учебному плану (090301, Информатика и вычислительная техника, профиль Автоматизированные системы обработки информации и управления)

Протокол заседания учебно-методической комиссии

от 09 июня 2021 г. № 11

Председатель учебно-методической комиссии ГИЭИ _____А.Г. Горбушин

Руководитель образовательной программы _____А.Г. Горбушин

21.05 2021г.

Аннотация к дисциплине

Название дисциплины	**Правовые основы информационной безопасности**
Направление подготовки (специальность)	**09.03.01 Информатика и вычислительная техника**
Направленность (профиль/программа/специализация)	Автоматизированные системы обработки информации и управления
Место дисциплины	Дисциплина относится к обязательной части Блока 1 «Дисциплины (модули)» ООП.
Трудоемкость (з.е. / часы)	3/108
Цель изучения дисциплины	Целью преподавания дисциплины является формирование способности принимать решения в профессиональной области с учетом требований информационной безопасности
Компетенции, формируемые в результате освоения дисциплины	УК-2- Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений ОПК-3- Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Содержание дисциплины (основные разделы и темы)	Информация как объект правовых отношений. Уровни правового обеспечения информационной безопасности; Основные законодательные акты в области защиты информации; Ответственность за нарушение режима информационной безопасности. Сущность и содержание организационных основ защиты информации. Правовой режим защиты государственной тайны и информации конфиденциального характера; Правовые основы лицензирования, сертификации и аттестации в области защиты информации; Правовые основы защиты персональных данных, ГИС (государственных информационных систем). Основные направления государственной политики по защите объектов КИИ.
Форма промежуточной аттестации	Зачет с оценкой

1. Цели и задачи дисциплины:

Целью освоения дисциплины является формирование способности принимать решения в профессиональной области с учетом требований информационной безопасности

Задачи дисциплины:

- изучение государственной политики в области защиты информации
- изучение основных нормативно-правовых актов, регламентирующих вопросы защиты информации
- получение навыков в применении нормативно-правовых актов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем

2. Планируемые результаты обучения

В результате освоения дисциплины у студента должны быть сформированы

Знания, приобретаемые в ходе освоения дисциплины

№ п/п	Знания
1	Государственной политики в области обеспечения информационной безопасности
2	Правовых основ защиты информации ограниченного доступа
3	Видов правонарушений и ответственности в области информационной безопасности

Умения, приобретаемые в ходе освоения дисциплины

№ п/п	Умения
1	Использовать правовые знания в области информационной безопасности в решении профессиональных задач

Навыки, приобретаемые в ходе освоения дисциплины

№ п/п	Навыки
1	В применении нормативно - правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем

Компетенции, приобретаемые в ходе освоения дисциплины

Компетенции	Индикаторы	Знания	Умения	Навыки
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической	ОПК-3.1 Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований	1,2	1	1

культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	информационной безопасности			
	ОПК-3.2 Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	1,2,3	1	1
	ОПК-3.3 Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	1,2,3	1	1
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Знать: виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы,регулирующие профессиональную деятельность	1,2,3	1	1
	УК-2.2 Уметь: проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты решений для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности	1,2,3	1	1
	УК-2.3 Владеть: методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией	1,2,3	1	

3. Место дисциплины в структуре ООП

Дисциплина относится к обязательной части Блока 1 «Дисциплины (модули)» ООПДисциплина изучается на 3 курсе в 5 семестре.

Изучение дисциплины базируется на знаниях, умениях и навыках, полученных при освоении дисциплин (модулей): Информатика, Правоведение

Перечень последующих дисциплин (модулей), для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной (модулем): "Защита информации", "Проектирование автоматизированных систем обработки информации и управления"

4. Структура и содержание дисциплины

4.1 Структура дисциплины

№ п/п	Раздел дисциплины. Форма промежуточн ой аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы					Содержание самостоятельной работы
				контактная				СРС	
				лек	пр	лаб	КЧА		
1	Введение. Основные направления государственной политики в области защиты информации	16	5	6	2	-		8	[1,2] Подготовка к устному опросу. Практическая работа. Подготовка к вопросам по практической работе
2	Основные понятия нормативно-правового обеспечения информационной безопасности	16	5	4	2	-		10	[1,2] Практическая работа. Подготовка к вопросам по практической работе
3	Правовые основы защиты государственной и коммерческой тайн.	20	5	6	4	-		10	[1,3] Практическая работа. Подготовка к вопросам по практической работе Подготовка к контрольной работе
4	Правовые основы лицензирования и сертификации в области защиты информации	10	5	2	2	-		6	[1,3] Практическая работа. Подготовка к вопросам по практической работе Подготовка к тестированию
5	Правовые основы защиты персональных данных, ГИС (государственных информационных систем), объектов КИИ (критической информационной инфраструктуры)	30	5	10	4	-		16	[1] Практическая работа. Подготовка к вопросам по практической работе
6	Нормативно – правовое обеспечение в сфере использования криптографических средств защиты информации	14	5	4	2	-		8	[1,3] Практическая работа. Подготовка к вопросам по практической работе
	Дифференцированный зачет	2	5	–	–	–	0,4	1,6	Зачет выставляется по совокупности результатов текущего контроля успеваемости
	Итого:	**108**		**32**	**16**	**-**	**0,4**	**59,6**	

4.2 Содержание разделов курса и формируемых в них компетенций

№ п/п	Раздел дисциплины	Коды компетенции и индикаторов	Знания	Умения	Навыки	Форма контроля
1	Введение. Основные направления государственной политики в области защиты информации	ОПК-3.1, ОПК-3.2, ОПК-3.3, УК-2.1, УК-2.2, УК-2.3	1,2,3	1	1	Устный опрос Практическое занятие
2	Основные понятия нормативно- правового обеспечения информационной безопасности	ОПК-3.1, ОПК-3.2, ОПК-3.3, УК-2.1, УК-2.2, УК-2.3	1,2,3	1	1	Практическое занятие
3	Правовые основы защиты государственной и коммерческой тайн.	ОПК-3.1, ОПК-3.2, ОПК-3.3, УК-2.1, УК-2.2, УК-2.3	1,2,3	1	1	Практические занятия. Контрольная работа
4	Правовые основы лицензирования и сертификации в области защиты информации	ОПК-3.1, ОПК-3.2, ОПК-3.3, УК-2.1, УК-2.2, УК-2.3	1,2,3	1	1	Практические занятия. Тест
5	Правовые основы защиты персональных данных, ГИС (государственных информационных систем), объектов КИИ (критической информационной инфраструктуры)	ОПК-3.1, ОПК-3.2, ОПК-3.3, УК-2.1, УК-2.2, УК-2.3	1,2,3	1	1	Практические занятия.
6	Нормативно – правовое обеспечение в сфере использования криптографических средств защиты информации	ОПК-3.1, ОПК-3.2, ОПК-3.3, УК-2.1, УК-2.2, УК-2.3	1,2,3	1	1	Практическое занятие

4.3 Наименование тем лекций, их содержание и объем вчасах

№ п/п	№ раздела дисциплины	Наименование лекций	Трудоем-кость (час)
1.	1	1. Цели и задачи курса. Основные понятия и определения. Национальные интересы и безопасность России. Доктрина информационной безопасности РФ. Стратегия развития информационного общества. 2. Государственная система защиты информации в РФ. Полномочия, права и обязанности органов государственной власти в области защиты информации.	6
2.	2	1. Правовые основы защиты информации. Уровни правового обеспечения информационной безопасности 2. Основные законодательные акты в области защиты информации 3. Информация как объект правовых отношений. 4. Категории информации по условиям доступа к ней 5. Ответственность за нарушение режима информационной безопасности	4

3.	3	1. Основные понятия в области защиты государственной тайны. Государственная система защиты гостайны в РФ. Межведомственная комиссия по защите гостайны. Грифы секретности в РФ. Порядок засекречивания и рассекречивания сведений, составляющих государственную тайну. Порядок допуска граждан и должностных лиц к государственной тайне 2. Правовые основы защиты коммерческой тайны. Порядок отнесения информации к коммерческой тайне.	6
	4	1. Лицензирование деятельности по защите информации ограниченного доступа и разработке и производству средств защиты информации 2. Сертификация средств защиты информации. Основные понятия и законодательное регулирование	2
	5	1. Законодательство в области защиты персональных данных 2. Классификация информационных систем персональных данных. Реализация мероприятий по защите персональных данных. Определение набора мер по защите персональных данных 3. Законодательство в области защиты государственных информационных систем 4. Классификация государственных информационных систем и требования к их защищенности 5. Основные требования законодательства к безопасности критической информационной инфраструктуры (КИИ) РФ. Классификация информационных систем КИИ.	10
	6	1. Нормативно – правовое обеспечение в сфере связи и криптографической защиты 2. Государственное регулирование вопросов использования криптографических средств и ЭЦП	4
	Всего		**32**

4.4 Наименование тем практических занятий, их содержание и объем в часах

№ п/п	№ раздела дисциплины	Наименование практических работ	Трудоем-кость (час)
1.	1	Анализ терминов и определений информационной безопасности . Национальные интересы РФ в области ИБ, приоритетные направления в области защиты информации. Органы, обеспечивающие национальную безопасность РФ	2
2.	2	Ответственность за правонарушения в области информационной безопасности	2
3.	3	Законодательство в области защиты государственной тайны. Перечень сведений, отнесенных к государственной тайне. Анализ нормативно -правовых документов в области защиты государственной тайны.	2
4.	3	Законодательство в области конфиденциальной информации. Анализ нормативно- правовых актов в области защиты коммерческой тайны. Ответственность за нарушение законодательства в области защиты коммерческой тайны. Составление нормативно-правовых актов в области защиты конфиденциальной информации на предприятии.	2
5.	4	Анализ и подбор сертифицированных средств защиты информации . Ответственность за использование несертифицированных СЗИ.	2

6.	5	Составления акта классификации информационной системы персональных данных. Классификация ГИС. Ответственность оператора персональных данных за нарушение законадательства.	2
7.	5	Анализ законодательства в области защиты КИИ. Категорирование объектов КИИ. Составление акта категорирования объекта КИИ	2
8.	6	Законодательство в области криптографической защиты информации. Ответственность в области криптографической защиты информации.	2
	Всего		**16**

4.5 Наименование тем лабораторных работ, их содержание и объем в часах

Лабораторные работы учебным планом не предусмотрены

5. Оценочные материалы для текущего контроля успеваемости и промежуточной аттестации по дисциплине

Для контроля результатов освоения дисциплины проводятся :

- контрольная работа
- тесты
- вопросы для устного опроса
- зачет

Примечание: оценочные материалы (типовые варианты тестов, контрольных работ и др.) приведены в приложении к рабочей программе дисциплины.

Промежуточная аттестация по итогам освоения дисциплины – зачет с оценкой

6. Учебно-методическое и информационное обеспечение дисциплины:

а) основная литература:

1. Нестеров С.А., Основы информационной безопасности [Электронный ресурс] : учебное пособие / Нестеров С.А.. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 c. — 978-5-7422-4331-1. — Режим доступа: http://www.iprbookshop.ru/43960.html

2. Галатенко, В. А. Основы информационной безопасности / В. А. Галатенко. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — ISBN 978-5-94774-821-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/52209.html

3. Краковский, Ю. М. Защита информации : учебное пособие / Ю. М. Краковский. — Ростов-на-Дону : Феникс, 2016. — 349 с. — ISBN 978-5-222-26911-4. — Текст : электронный

// Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/59350.html

б) дополнительная литература:

4. Быкадоров, В. А. Техническое регулирование и обеспечение безопасности [Электронный ресурс] : учебное пособие для студентов вузов, обучающихся по специальности «Юриспруденция» / В. А. Быкадоров, Ф. П. Васильев, В. А. Казюлин ; под ред. Ф. П. Васильев. — Электрон. текстовые данные. — М. : ЮНИТИ-ДАНА, 2014. — 639 c. — 978-5- 238-02537-7. — Режим доступа: http://www.iprbookshop.ru/21004.html

г) перечень ресурсов информационно-коммуникационной сетиИнтернет:

1. Электронно-библиотечная система IPRbookshttp://istu.ru/material/elektronno-bibliotechnaya-sistema-iprbooks.
2. Электронный каталог научной библиотеки ИжГТУ имени М.Т. Калашникова Web ИРБИС http://94.181.117.43/cgi-bin/irbis64r_12/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=IBIS&P21DBN= IBIS.
3. Национальная электронная библиотека –http://нэб.рф.
4. Мировая цифровая библиотека –http://www.wdl.org/ru/.
5. Международный индекс научного цитирования WebofScience – http://webofscience.com.
6. Научная электронная библиотека eLIBRARY.RU – https://elibrary.ru/defaultx.asp.
7. Справочно-правовая системаКонсультантПлюсhttp://www.consultant.ru/.

д) лицензионное и свободно распространяемое программноеобеспечение:

1. LibreOffice (свободно распространяемое ПО)
2. Doctor Web (лицензионное ПО)

7. Материально-техническое обеспечение дисциплины:

1. Лекционные занятия .

Учебные аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно- наглядные пособия, тематические иллюстрации – *при необходимости*).

2. Практические занятия .

Учебные аудитории для практических занятий укомплектованы специализированноймебелью и техническими средствами обучения (проектор, экран, компьютер/ноутбук – *при необходимости*).

Для практических занятий используются аудитория, оснащенная следующимоборудованием:

Компьютеры с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде ИжГТУ имени М.Т. Калашникова

3. Самостоятельная работа.

Аудитория № 204, 205, 206, 209, оснащенная следующим оборудованием: столы лабораторные, стулья, компьютерная техника с возможностью подключения к сети «Интернет».

1. Самостоятельная работа.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно- образовательной среде ИжГТУ имени М.Т. Калашникова:

- научная библиотека ИжГТУ имени М.Т. Калашникова;
- помещение для самостоятельной работы обучающихся.

При необходимости рабочая программа дисциплины (модуля) может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для обучения с применением дистанционных образовательных технологий. Для этого требуется заявление студента (его законного представителя) и заключение психолого- медико-педагогической комиссии (ПМПК).

МИНОБРНАУКИ РОССИИ
Глазовский инженерно-экономический институт (филиал)
Федерального государственного бюджетного образовательного
учреждения высшего образования
«Ижевский государственный технический университет
имени М.Т. Калашникова»
(ГИЭИ (филиал) ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)

Оценочные средствапо дисциплине

Правовые основы информационной безопасности

наименование – полностью

направление 09.03.01 «Информатика и вычислительная техника»

профиль Автоматизированные системы обработки информации и управления

уровень образования: бакалавриат

форма обучения: очная

очная/очно-заочная/заочная

общая трудоемкость дисциплины составляет: 3 зачетные единиц(ы)

1. Оценочные средства

Оценивание формирования компетенций производится на основе результатов обучения, приведенных в п. 2 рабочей программы и ФОС. Связь разделов компетенций, индикаторов и форм контроля (текущего и промежуточного) указаны в таблице 4.2 рабочей программы дисциплины.

Оценочные средства соотнесены с результатами обучения по дисциплине и индикаторами достижения компетенций, представлены ниже.

№ п/п	Коды компетенции и индикаторов	Результат обучения *(знания, умения и навыки)*	Формы текущего и промежуточного контроля
1	ОПК-3.1 Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	З1. Государственной политики в области обеспечения информационной безопасности З2. Правовых основ защиты информации ограниченного доступа У1..Использовать правовые знания в области информационной безопасности в решении профессиональных задач Н1. В применении нормативно - правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Устный опрос Практические работы Контрольная работа тестирование Зачет
	ОПК-3.2 Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	З1. Государственной политики в области обеспечения информационной безопасности З2. Правовых основ защиты информации ограниченного доступа З3. Видов правонарушений и ответственности в области информационной безопасности У1..Использовать правовые знания в области информационной безопасности в решении профессиональных задач Н1. В применении нормативно - правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Устный опрос Практические работы Контрольная работа тестирование Зачет
	ОПК-3.3 Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с	З1. Государственной политики в области обеспечения информационной безопасности З2. Правовых основ защиты информации ограниченного	Устный опрос Практические работы Контрольная работа тестирование Зачет

	учетом требований информационной безопасности	доступа З3. Видов правонарушений и ответственности в области информационной безопасности У1..Использовать правовые знания в области информационной безопасности в решении профессиональных задач Н1. В применении нормативно - правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	
2	УК-2.1 Знать: виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность	З1. Государственной политики в области обеспечения информационной безопасности З2. Правовых основ защиты информации ограниченного доступа З3. Видов правонарушений и ответственности в области информационной безопасности У1..Использовать правовые знания в области информационной безопасности в решении профессиональных задач Н1. В применении нормативно - правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Устный опрос Практические работы Контрольная работа тестирование Зачет
	УК-2.2 Уметь: проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты решений для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности	З1. Государственной политики в области обеспечения информационной безопасности З2. Правовых основ защиты информации ограниченного доступа З3. Видов правонарушений и ответственности в области информационной безопасности У1..Использовать правовые знания в области информационной безопасности в решении профессиональных задач Н1. В применении нормативно - правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Устный опрос Практические работы Контрольная работа тестирование Зачет
	УК-2.3 Владеть: методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с	З1. Государственной политики в области обеспечения информационной безопасности З2. Правовых основ защиты информации ограниченного	Устный опрос Практические работы Контрольная работа тестирование Зачет

	нормативно-правовой документацией	доступа З3. Видов правонарушений и ответственности в области информационной безопасности У1..Использовать правовые знания в области информационной безопасности в решении профессиональных задач Н1. В применении нормативно - правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	

Наименование: дифференцированный зачет

***Представление в ФОС*:**
Перечень вопросов для проведения зачета:

1. Основные понятия в области защиты информации. Определение и сравнение терминов «информационная безопасность» и «защита информации»
2. Роль и место ИБ в системе национальной безопасности государства
3. Государственная политика обеспечения ИБ в РФ
4. Права, полномочия и обязанности Президента РФ, Правительства РФ и др. федеральных и муниципальных органов исполнительной власти субъектов РФ в области безопасности
5. Полномочия, задачи, функции и права ФСБ в области защиты информации
6. Полномочия, задачи, функции и права ФСТЭК в области защиты информации
7. Полномочия, обязанности и права Федеральной службы по надзору в сфере связи, массовых коммуникаций и информационных технологий в области защиты информации при обработке персональных данных
8. Информация как объект правовых отношений. Характеристика информационного права
9. Уровни правового обеспечения ИБ. Иерархия нормативных актов в области защиты информации. Сущность и содержание основных нормативно-правовых актов в области ИБ
10. Ответственность за правонарушения в области ИБ
11. Сущность основных понятий в области защиты государственной тайны.
12. Государственная система защиты гостайны, органы защиты гостайны.
13. Межведомственная комиссия по защите гостайны и ее основные задачи в области защиты гостайны.
14. Допуск граждан к государственной тайне. Порядок оформления допуска к гостайне.
15. Правовые основы защиты коммерческой тайны. Понятия «коммерческая тайна», «режим коммерческой тайны»
16. Порядок отнесения информации к коммерческой тайне
17. Права обладателя информации, составляющей коммерческую тайну.
18. Ответственность за нарушение режима коммерческой тайны.
19. Способы охраны конфиденциальной информации. ФЗ «О коммерческой тайне»
20. Цели и задачи и принципы в области лицензирования
21. Полномочия и права лицензирующих органов в области информационной безопасности
22. Процедура получения лицензии. Срок действия лицензии
23. Сертификация в РФ. Процедура сертификации средств защиты информации. Срок

действия сертификата.

24. Ответственность за правонарушение в области лицензирования и сертификации
25. Законодательство в области защиты персональных данных
26. Порядок классификации информационных систем персональных данных.
27. Реализация мероприятий по защите персональных данных.
28. Права и обязанности оператора, обрабатывающего персональные данные
29. Права и обязанности субъекта персональных данных
30. Основные требования законодательства к безопасности критической информационной инфраструктуры (КИИ) РФ. Классификация информационных систем КИИ
31. Законодательство в области криптографии и связи
32. Государственное регулирование вопросов использования ЭП. Виды и назначение ЭП
33. Доктрина информационной безопасности Российской Федерации от 05.12.2016г. и ее краткая характеристика
34. Государственная программа Российской Федерации " О стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" и ее краткая характеристика
35. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и его краткая характеристика
36. Федеральный закон «О коммерческой тайне» и его краткая характеристика
37. Закон РФ от 21 июля 1993 г. № 5485-I «О государственной тайне» и его краткая характеристика
38. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и его краткая характеристика
39. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и его краткая характеристика
40. Статья 272 УК РФ (Неправомерный доступ к компьютерной информации). Рассмотреть по составу.
41. Статья 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ). Рассмотреть по составу.
42. Статья 274 УК РФ (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей). Рассмотреть по составу.
43. Статья 183 УК РФ (Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну).
44. Статья 13.12 КоАП РФ. Нарушение правил защиты информации
45. Статья 13.13 КоАП РФ. Незаконная деятельность в области защиты информации
46. Статья 13.14 КоАП РФ. Разглашение информации с ограниченным доступом

Критерии оценки:

Приведены в разделе 2

Наименование: тест

Варианты тестов:

1. **Какие из утверждений является верными**

а)сертифицирует средства СЗИ ,выдают сертификаты и лицензии на применение знака соответствия с представлением копий в федеральные органы по сертификации и ведут учет

б)не имеют права представлять по их требованию необходимую информацию

в)имеет право приостанавливать либо обменять действие выданных ими сертификатов и лицензий на применение знака соответствия

2. Какие центры по сертификации находятся в УР(г.Ижевск)
а)Softjet

б)Иж-стандарт
в)НПО Компьютер
г)УЦС

3. Участником сертификации средств защиты информации нижеперечисленных являются
а)федеральный орган по сертификации
б)ФСБ

в)ФСТЭК

г)испытательные лаборатории
д)изготовители-продавцы

4. Каких категорий обьектов не существует
а)особоважный обьект
б)секретный обьект
в)режимный обьект
г)особорежимный обьект

5. Комплекс мероприятий подтверждает, что обьект соответствует требованиям стандартов и иных нормативых документов утвержд. ФСТЭК РФ
а)аттестация обьекта
б)организация обьекта
в)лицензирование обьекта

6. Центральный орган системы сертификации:
а)организует работы по формированию систем сертификации
б)координирует деятельность органов

в)ведет учет входящих в систему сертификации органов по сертификации средств ЗИ
г)все варианты верны

7. федеральный орган по сертификации в пределах своей компенсации
а)создает систему сертификации

б)осуществляет выбор способа подтвержления соответствия средств ЗИ и требования нормативных документов

в)выдает сертификат и лицензию на применеие знака соответствия
г)все варианты верны

8. Сколько выделяют зон безопасности внутри обьекта
а)4

б)6

в)9

г)3

9. К федеральным органам по сертификации относятся
а)ФСТЭК
б)ФСБ

в)Министерство Обороны РФ
г)ГТК

10. Обязательной аттестации подлежат обьекты информатизации
а)коммерческая тайна
б)гос .тайна

в)ведение секретных переговоров
г)нет верного ответа

11. Что поверяет ФСТЭК у сертифицированных продуктов
а)**галографическая наклейка**
б)ПО

в)паспорт на продукт
г)Все правильно

12. Укажите, что определяют соответствующие госорганы в области сертификации

а)порядок выдачи и приостановки сертификатов б)порядок оплаты услуг по сертификации

в)права и обязанности участника системы сертификации с ЗИг)все правильно

Критерии оценки:

Приведены в разделе 2

Наименование: контрольная работа
Представление в ФОС*:** набор вариантов заданийВарианты заданий:***

1) Назовите грифы секретности материальных носителей
2) Назовите формы допуска сотрудников к гостайне
3) Опишите как сведения становятся гостайной
4) Что такое гриф секретности и куда он наносится?
5) Укажите срок засекречивания материальных носителей
6) Какие функции выполняет Межведомственная комиссия
7) Опишите условия для получения формы допуска к ГТ
8) Срок действия допуска к ГТ?
9) Кто проводит проверочные мероприятия по допуску сотрудника к ГТ?
10) Что такое перечень сведений, отнесенных к ГТ на предприятии, кто его разрабатывает.Актуализирует?
11) Какие ограничения могут быть наложены на сотрудника с допуском ГТ?
12) Какие преференции имеет сотрудник с допуском ГТ?
13) «СС» - это гриф к сведениям в какой области?
14) Кто имеет права допуска к ГТ без его оформления?
15) Министр УР по информатизации – имеет права допуска к ГТ без оформления?
16) Глава УР имеет права допуска к ГТ без оформления?

Критерии оценки:

Приведены в разделе 2

Наименование: устный опрос

***Представление в ФОС*:** перечень заданий или вопросов

Варианты заданий:

Задание №1. Проанализируйте Стратегию развития информационного обществана 2017-2030г. Ответьте на вопросы:

- *Стратегия развития общества на 2017-2030 г. основные цели и ее отличие от Стратегииразвитии общества от 7.02.2008г. (№Пр-212)?*

Задание №2. Объясните следующие понятия:

- *Безопасное ПО?*
- *Интернет вещей?*
- *Критическая информационная инфраструктура?*
- *Облачные вычисления, туманные вычисления?*
- *Приведите примеры объектов с критической информационной инфраструктурой?*
- *Информационное пространство? Информационное общество? Цифровая экономика? Электронное правительство?*
- *Индустриальный интернет?*

Критерии оценки:
Приведены в разделе 2

Наименование: практические работы ***Представление в ФОС*:** набор вариантов заданий ***Варианты заданий:***

- Познакомиться с нормативной базой по допуску граждан к ГТ
- Оформить карточку допуска (форма 1) (ознакомиться с формой карточки и выписатьосновные данные, которые необходимы для заполнения карточки допуска)
- **Ответить на вопросы**:
- 1)Кто проводит проверочные мероприятия?
- 2) Могут ли запрашивать при проверочных мероприятиях сведения, касающиеся личной исемейной тайны?
- 3) Нужно ли оформлять допуск гражданину для работы с информацией грифа «Служебнаятайна»

Критерии оценки:
Приведены в разделе 2

2. Критерии и шкалы оценивания

Для контрольных мероприятий (текущего контроля) устанавливается минимальное и максимальное количество баллов в соответствии с таблицей. Контрольное мероприятие считается пройденным успешно при условии набора количества баллов не ниже минимального.

Результат обучения по дисциплине считается достигнутым при успешном прохождении обучающимся всех контрольных мероприятий, относящихся к данному результату обучения.

Разделы дисциплины	***Форма контроля***	***Количество баллов***	
		min	***max***
1	Устный опрос	3	5
1	Выполнение практической работы, ответ на вопросы	7	10
2	Выполнение практической работы, ответ на вопросы	7	10

3	Выполнение практической работы, ответ на вопросы	7	10
3	Выполнение практической работы, ответ на вопросы	6	10
3	Контрольная работа	5	10
4	Выполнение практической работы, ответ на вопросы	5	10
4	тест	5	10
5	Выполнение практической работы, ответ на вопросы	5	7
5	Выполнение практической работы, ответ на вопросы	5	8
6	Выполнение практической работы, ответ на вопросы	5	10

При оценивании результатов обучения по дисциплине в ходе текущего контроля успеваемости используются следующие критерии. Минимальное количество баллов выставляется обучающемуся при выполнении всех показателей, допускаются несущественные неточности в изложении и оформлении материала.

Наименование, обозначение	***Показатели выставления минимального количества баллов***
Практическая работа	Задания выполнены более чем наполовину. Присутствуют серьёзные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий. На защите практической работы даны правильные ответы не менее чем на 50% заданных вопросов
Контрольная работа	Продемонстрирован удовлетворительный уровень владения материалом. Правильно решено не менее 50% заданий
Тест	Правильно решено не менее 50% тестовых заданий
Устный опрос	Даны правильные ответы не менее чем на 50% заданных вопросов. Продемонстрированы знания основного учебно-программного материала

Промежуточная аттестация по дисциплине проводится в форме дифференцированного зачета. Итоговая оценка выставляется с использованием следующей шкалы.

Оценка	***Набрано баллов***
«отлично»	88-100
«хорошо»	76-87
«удовлетворительно»	61-75
«неудовлетворительно»	менее 60

При оценивании результатов обучения по дисциплине в ходе промежуточной аттестации используются следующие критерии и шкала оценки:

Оценка	***Критерии оценки***
«отлично»	Обучающийся показал всестороннее, систематическое и глубокое знание учебного материала, предусмотренного программой, умение уверенно применять на их практике при решении задач (выполнении заданий), способность полно, правильно и аргументировано отвечать на вопросы и делать необходимые выводы. Свободно использует основную литературу и знаком с дополнительной литературой, рекомендованной программой

«хорошо»	Обучающийся показал полное знание теоретического материала, владение основной литературой, рекомендованной в программе, умение самостоятельно решать задачи (выполнять задания), способность аргументировано отвечать на вопросы и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя. Способен к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности
«удовлетворительно»	Обучающийся демонстрирует неполное или фрагментарное знание основного учебного материала, допускает существенные ошибки в его изложении, испытывает затруднения и допускает ошибки при выполнении заданий (решении задач), выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов. Владеет знанием основных разделов, необходимых для дальнейшего обучения, знаком с основной и дополнительной литературой, рекомендованной программой
«неудовлетворительно»	Обучающийся при ответе демонстрирует существенные пробелы в знаниях основного учебного материала, допускает грубые ошибки в формулировании основных понятий и при решении типовых задач (при выполнении типовых заданий), не способен ответить на наводящие вопросы преподавателя. Оценка ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании образовательного учреждения без дополнительных занятий по рассматриваемой дисциплине