МИНОБРНАУКИ РОССИИ

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



ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 3DA273AA38C240BA869FA062FFFB332C
Владелец: Золотов Алексей Васильевич
Действителен: с 29.07.2026 до 22.10.2027

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Правовые основы информационной безопасности

направление подготовки: **09.03.01 «Информатика и вычислительная техника»**

направленность (профиль): **Автоматизированные системы обработки информации и управления**

уровень образования: **бакалавриат**

форма обучения: **очная**

общая трудоемкость дисциплины составляет: **3 зачетных единиц**

Кафедра «Машиностроение и информационные технологии»

Составитель:

Рабочая программа составлена в соответствии с требованиями федерального государственногообразовательного стандарта высшего образования по направлению подготовки 09.03.01 «Информатика и вычислительная техника» и рассмотрена на заседании кафедры.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.01 «Информатика и вычислительная техника» и рассмотрена на заседании кафедры.

Протокол от 22.05.2023 г. № 5

Заведующий кафедрой  А.Г. Горбушин

22.05.2023 г.

СОГЛАСОВАНО

Количество часов рабочей программы и формируемые компетенции соответствуют учебному плану по направлению подготовки 09.03.01 «Информатика и вычислительная техника», профиль «Автоматизированные системы обработки информации и управления».

Протокол заседания учебно-методической комиссии от 22 мая 2023 г. № 2

Председатель учебно-методической комиссии ГИЭИ

 А.Г. Горбушин

Руководитель образовательной программы  А.Г. Горбушин

22.05.2023 г.

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 з.е./108 час.
Цель изучения дисциплины	Формирование способности принимать решения в профессиональной области с учетом нормативно-правовых требований информационной безопасности
Компетенции, формируемые в результате освоениядисциплины	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; 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
Содержание дисциплины (основные разделы итемы)	Основные направления государственной политики в области защиты информации. Основные понятия нормативно- правового обеспечения информационной безопасности. Ответственность за нарушение режима информационной безопасности. Правовые основы защиты государственной и коммерческой тайн. Правовые основы лицензирования и сертификации в области защиты информации. Правовые основы защиты персональных данных, ГИС (государственных информационных систем), объектов КИИ (критической информационной инфраструктуры). Нормативно – правовое обеспечение в сфере использования криптографических средств защиты информации
Форма промежуточной аттестации	Зачет с оценкой (5 семестр)

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

№	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

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

Навыки, приобретаемые в ходе освоения дисциплины

№	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 культуры с применением информационно-коммуникационных технологий и с учетом	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	1,2	1	1

основных требований 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	1

3. Место дисциплины в структуре ООП

Дисциплина относится к обязательной части Блока 1 «Дисциплины (модули)» ООП

Дисциплина изучается на 3 курсе в 5 семестре.

Изучение дисциплины базируется на знаниях, умениях и навыках, полученных при освоении дисциплин (модулей): Информационные технологии, 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 *(по семестрам)*	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы					Содержание самостоятельной работы
				контактная				СРС	
				лек	пр	лаб	КЧА		
1	2	3	4	5	6	7	8	10	11
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)	32	5	12	4	-		16	[1] Практическая работа. Подготовка к вопросам по практической работе
6	Нормативно – правовое обеспечение в сфере использования криптографических средств защиты информации	12	5	2	2	-		8	[1,3] Практическая работа. Подготовка к вопросам по практической работе

	Зачет с оценкой	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.
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 в часах

№ 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	4

		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	
3.	3	1. Основные понятия в области защиты государственной тайны. Государственная система защиты гостайны в РФ. 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. Определение набора мер по защите персональных данных. Государственный контроль операторов персональных данных по выполнению требований законодательства 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.	12
	6	1. Нормативно – правовое обеспечение в сфере связи и криптографической защиты 2. Государственное регулирование вопросов использования криптографических средств и ЭЦП	2
	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	2

		законодательства в области защиты коммерческой тайны. Составление нормативно-правовых актов в области защиты конфиденциальной информации на предприятии.	
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 законодательства.	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 :

- 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. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/97562.html
2. Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гультяева. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/91640.html
3. Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. — Москва, Вологда : Инфра-Инженерия, 2022. — 104 с. — ISBN 978-5-9729-0864-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/124242

б) дополнительная литература:

1. Информационная безопасность. Практические аспекты : учебник для вузов / Л. Х. Сафиуллина, А. Р. Касимова, Я. С. Рябов [и др.]. — Санкт-Петербург : Интермедия, 2021. — 240 с. — ISBN 978-5-4383-0205-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL:

https://www.iprbookshop.ru/103997

г) перечень ресурсов информационно-коммуникационной сети Интернет:

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. Научнаяэлектронная библиотека eLIBRARY.RU – https://elibrary.ru/defaultx.asp.
7. Справочно-правовая система КонсультантПлюсhttp://www.consultant.ru/.

д) лицензионное и свободно распространяемое программное обеспечение:

1. Офисный пакет MS Office

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 специализированной мебелью и техническими средствами обучения (проектор, экран, компьютер/ноутбук – *при необходимости*).

Для практических занятий используются аудитория № 2, оснащенная следующим оборудованием:

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

3. Самостоятельная работа.

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

- научная библиотека ИжГТУ имени М.Т. Калашникова;
- помещения 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
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»

Оценочные средства
по 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 единицы

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	Устный опрос Практические работы 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	У1..Использовать правовые знания в области информационной безопасности в решении профессиональных задач	Устный опрос Практические работы тестирование Зачет
	ОПК-3.3 Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Н1. В применении нормативно - правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Устный опрос Практические работы тестирование Зачет

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	Устный опрос Практические работы 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	У1..Использовать правовые знания в области информационной безопасности в решении профессиональных задач	Устный опрос Практические работы тестирование Зачет
	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	Н1. В применении нормативно - правовых актов и разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Устный опрос Практические работы тестирование Зачет

Наименование: зачет с оценкой
***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. Права, полномочия и обязанности Президента РФ, Правительства РФ и др. федеральных и муниципальных органов исполнительной власти субъектов РФ в области безопасности
4. Полномочия, задачи, функции и права ФСБ в области защиты информации
5. Полномочия, задачи, функции и права ФСТЭК в области защиты информации
6. Информация как объект правовых отношений. Характеристика информационного права
7. Уровни правового обеспечения ИБ. Иерархия нормативных актов в области защиты информации. Сущность и содержание основных нормативно-правовых актов в области ИБ
8. Ответственность за правонарушения в области ИБ
9. Сущность основных понятий в области защиты государственной тайны.

10. Государственная система защиты гостайны, органы защиты гостайны.
11. Допуск граждан к государственной тайне. Порядок оформления допуска к гостайне.
12. Правовые основы защиты коммерческой тайны. Понятия «коммерческая тайна», «режим коммерческой тайны»
13. Порядок отнесения информации к коммерческой тайне
14. Права обладателя информации, составляющей коммерческую тайну.
15. Ответственность за нарушение режима коммерческой тайны.
16. Лицензирование в области защиты информации. Срок действия лицензии.
17. Сертификация в РФ. Процедура сертификации средств защиты информации. Срок действия сертификата.
18. Ответственность за правонарушение в области лицензирования и сертификации
19. Законодательство в области защиты персональных данных
20. Порядок классификации информационных систем персональных данных.
21. Реализация мероприятий по защите персональных данных.
22. Права и обязанности оператора, обрабатывающего персональные данные
23. Права и обязанности субъекта персональных данных
24. Основные требования законодательства к безопасности критической информационной инфраструктуры (КИИ) РФ. Классификация информационных систем КИИ
25. Законодательство в области криптографии и связи
26. Государственное регулирование вопросов использования ЭП. Виды и назначение ЭП
27. Доктрина информационной безопасности Российской Федерации от 05.12.2016г. и ее краткая характеристика
28. Государственная программа Российской Федерации " О стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" и ее краткая характеристика
29. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и его краткая характеристика
30. Федеральный закон «О коммерческой тайне» и его краткая характеристика
31. Закон РФ от 21 июля 1993 г. № 5485-I «О государственной тайне» и его краткая характеристика
32. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и его краткая характеристика
33. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и его краткая характеристика
34. Статья 272 УК РФ (Неправомерный доступ к компьютерной информации). Рассмотреть по составу.
35. Статья 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ). Рассмотреть по составу.
36. Статья 274 УК РФ (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей). Рассмотреть по составу.
37. Статья 183 УК РФ (Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну).
38. Статья 13.12 КоАП РФ. Нарушение правил защиты информации
39. Статья 13.13 КоАП РФ. Незаконная деятельность в области защиты информации

Критерии оценки:

Приведены в разделе 2

При проведении диагностики освоения компетенций и оценки минимального уровня знаний могут

быть использованы тестовые материалы

Наименование: тест
Представление в ФОС: перечень заданий

1) Основные направления в области политики информационной безопасности определяются:
1) Федеральным Собранием Российской Федерации
2) Президентом Российской Федерации
3) Государственной Думой Российской Федерации
4) Правительством Российской Федерации

2. Доктрина информационной безопасности Российской Федерации это:
a) система положений о правилах информационной безопасности предприятия
b) система официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере
c) система требований по защите конфиденциальной информации
d) система рекомендаций по разработке политики безопасности на предприятии

3) **Регуляторами в области ИБ являются (несколько вариантов):**
1) Минцифры России
2) ФСБ
3) ФСТЭК
4) Росприроднадзор
5) Роскомнадзор
6) Гостехкомиссия

4) Доступ к информации – это
1) Возможность получения информации и ее использования;
2) Возможность использования информации;
3) Возможность доступа к информации;
4) Возможность доступа к информации, но не ее использования;

5) Какую область отношений регулирует ФЗ №152?
1) О коммерческой тайне
2) О технических требованиях по ИБ
3) О персональных данных
4) Нет такого ФЗ

6) Что нельзя отнести к коммерческой тайне?
1) Зарплаты сотрудников коммерческой организации
2) Используемые технологии промышленного производства
3) Влияние деятельности организации на окружающую среду
4) Используемые в организации ТСО (технические средства охраны)

7) Назовите гриф секретности, который не используется в режиме гос.тайны:
1) Секретно
2) Совершенно секретно
3) Для служебного пользования
4) Особой важности

8) Под безопасным ПО понимается:
1) ПО, разработанное на территории РФ
2) ПО, имеющее лицензию разработчика

3) ПО, сертифицированное ФСБ и(или) ФСТЭК
4) ПО, протестированное на отсутствие не декларированных возможностей
5) ПО, протестированное на уязвимости кода

9) **Объектом КИИ <u>не является</u> автоматизированная система, функционирующая в области:**
1) Здравоохранения
2) Образования
3) Транспорта
4) Оборонной промышленности
5) Кредитно-финансовой сфере

10) Электронная подпись согласно Федеральному закону от 06.04.2011 №63-ФЗ «Об электронной подписи», подразделяется на:
1. доверенную электронную подпись
2. простую электронную подпись;
3. неквалифицированную электронную подпись;
4. главную электронную подпись

квалифицированную электронную подпись.

Ключи теста:

№ вопроса	1	2	3	4	5	6	7	8	9	10
Ответ	2	2	2,3,5	1	2	2	2	2	3	2,3,5

1. Какой нормативно-правовой акт является специальным в области противодействия коррупции:
1. от 29.12.2012 № 273-ФЗ;
2. от 25.12.2008 № 273-ФЗ;
3. от 07.02.2011 № 3-ФЗ;
4. от 06.10.2003 № 131-ФЗ.

2. Согласно Российского законодательства под коррупцией понимается незаконное использование физическим лицом своего должностного положения в целях получения выгоды в интересах:
1. себя;
2. юридического лица;
3. третьих лиц;
4. все варианты верны.

3. Какие нормативно-правовые акты составляют правовую базу в сфере противодействия коррупции в Российской Федерации:
1. Конституция РФ;
2. нормы международного права;
3. муниципальные акты;
4. все варианты верны.

4. Под конфликтом интересов понимается личная заинтересованность лица, которая влияет или может повлиять на надлежащее исполнение должностных служебных обязанностей в интересах себя или лиц, находящихся по отношении к нему:
1. в близком родстве;
2. в свойственных отношениях;
3. в близких отношениях;
4. все варианты верны.

5. Обязанность по предупреждению коррупции возложена на:
1. государственные и муниципальные организации;
2. организации любых форм собственности;
3. акционерные общества;
4. общества с ограниченной ответственностью.

6. В каком из нормативно правовых актов отражены ограничения для государственных гражданских служащих:
1. Конституция РФ;
2. Федеральный закон от 27.07.2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;
3. Федеральный закон от 27.05.2003 г. № 58 «О системе государственной службы Российской Федерации»;
4. Указ Президента РФ от 31.12.2005 г. № 1574 «О реестре должностей федеральной государственной гражданской службы».

7. В какой из нормативно-правовых актов содержится правила этикета дарения и получения подарков государственными гражданскими служащими:
1. Конституция РФ от 1993 г.;
2. Федеральный закон от 27.07.2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;
3. Федеральный закон от 27.05.2003 г. № 58 «О системе государственной службы Российской Федерации»;
4. Конституция РФ от 2020 г..

8. К коррупции относится:
1. все указанное верно;
2. коммерческий подкуп;
3. дача взятки;
4. злоупотребление служебным положением.

9. Непринятие государственным гражданским служащим, являющимся стороной конфликта интересов, мер по предотвращению или урегулированию конфликта интересов является правонарушением влекущим:
1. применение к государственному гражданскому служащему мер уголовной ответственности;
2. применение к государственному гражданскому служащему мер гражданско-правовой ответственности;
3. применение к государственному гражданскому служащему мер дисциплинарной ответственности;
4. применение к государственному гражданскому служащему мер административной ответственности.

10. Сведения о доходах, расходах, об имуществе и обязательствах имущественного характера предоставляются государственными гражданскими служащими по форме справки, утвержденной:
1. Президентом Российской Федерации;
2. Правительством Российской Федерации;
3. федеральным органом исполнительной власти Российской Федерации, в котором государственный гражданский служащий проходит государственную гражданскую службу;
4. Федеральным Собранием Российской Федерации.

11. В какой срок должны быть размещены на официальном сайте государственного органа

сведения о декларированном годовом доходе федерального государственного служащего и членов его семьи:
1. в течение 14 рабочих дней со дня истечения срока, установленного для подачи справок о доходах, об имуществе и обязательствах имущественного характера;
2. в течение 14 календарных дней со дня истечения срока, установленного для подачи справок о доходах, об имуществе и обязательствах имущественного характера;
3. в течение 7 рабочих дней со дня истечения срока, установленного для подачи справок о доходах, об имуществе и обязательствах имущественного характера;
4. в течение 7 календарных дней со дня истечения срока, установленного для подачи справок о доходах, об имуществе и обязательствах имущественного характера.

12. При заполнении справки о доходах, об имуществе и обязательствах имущественного характера в числе прочего государственный гражданский служащий обязан представлять сведения о следующих видах транспортных средств:
1. принадлежащих родителям государственного гражданского служащего;
2. принадлежащих государственному гражданскому служащему в связи с исполнением должностных обязанностей;
3. за которые государственным гражданским служащим в отчетном периоде была оформлена предоплата, но при этом право собственности на государственного гражданского служащего оформлено не было;
4. находящихся в собственности государственного гражданского служащего.

13. В случае, если в ходе осуществления контроля за расходами государственного гражданского служащего выявлено несоответствие расходов служащего и членов его семьи их доходам:
1. органы прокуратуры обращаются в суд с иском об обращении в доход государства имущества, законность приобретения которого государственный гражданский служащий не может обосновать;
2. органы прокуратуры обращаются в суд с иском о применении к государственному служащему мер уголовной ответственности;
3. государственный служащий получает строгий выговор;
4. государственный служащий незамедлительно увольняется с государственной службы.

14. Невыполнение государственным гражданским служащим обязанности представлять представителю нанимателя сведения о доходах, расходах, об имуществе и обязательствах имущественного характера влечет:
1. привлечение к уголовной ответственности в соответствии с законодательством Российской Федерации;
2. освобождение государственного гражданского служащего от занимаемой должности государственной гражданской службы, увольнение его с государственной гражданской службы;
3. освобождение государственного гражданского служащего от занимаемой должности государственной гражданской службы;
4. привлечение к административной ответственности в соответствии с законодательством Российской Федерации.

15. В случае, если сведения о доходах, об имуществе и обязательствах имущественного характера государственного гражданского служащего размещены в информационно-телекоммуникационной сети «Интернет» на официальном сайте государственного органа, данные сведения для средств массовой информации:
1. не предоставляются;
2. предоставляются для опубликования в порядке, определяемом законодательством;
3. могут быть предоставлены по усмотрению руководителя государственного органа предоставляются только в отношении руководителей государственных органов;
4. предоставляются свободно.

Ключи теста:

Вопрос	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.
Ответ	2	4	4	4	2	2	2	1	3	1	1	4	1	2	2

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 Стратегии развитии 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 выписать основные 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 и семейной тайны?
- 3) Нужно ли оформлять допуск гражданину для работы с информацией грифа «Служебная тайна»

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	5	10
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
4	Выполнение практической работы, ответ на вопросы	6	10
4	тест	6	10
5	Выполнение практической работы, ответ на вопросы	6	10
5	Выполнение практической работы, ответ на вопросы	5	10
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
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 зачета с оценкой
Итоговая оценка выставляется с использованием следующей шкалы.

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

Если сумма набранных баллов менее 60– обучающийся не допускается до промежуточной аттестации.

Если сумма баллов составляет от 60 до 100 баллов – обучающийся допускается до зачета, при условии что выполнены и защищены контрольные работы.

По сумме набранных баллов студенту может быть выставлена оценка за промежуточную аттестацию, согласно приведенной шкале. Обучающийся имеет право сдать зачет в письменной форме для изменения балла

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