МИНОБРНАУКИ РОССИИ
Воткинский филиал
Федерального государственного бюджетного образовательного
учреждения высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»
(ВФ ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)

УТВЕРЖДАЮ
Директор
_____/Давыдов И.А.
__03 июня____ 2020_ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Правовые основы информационной безопасности

направление 09.03.01 «Информатика и вычислительная техника»

профиль «Автоматизированные системы обработки информации и управления»

уровень образования: бакалавриат

форма обучения: очная

общая трудоемкость дисциплины составляет: ___3___ зачетных единиц(ы)

Кафедра Естественные науки и информационные технологии

Составитель _____

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

Протокол от __03 июня__ 2020 г. № 4

Заведующий кафедрой _____К.Б. Сентяков

__03 июня__ 2020 г.

СОГЛАСОВАНО

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

Председатель учебно-методической комиссии по направлению 09.03.01 «Информатика и вычислительная техника», профиль «Автоматизированные системы обработки информации и управления»

_____К.Б. Сентяков

__03 июня__ 2020 г.

Руководитель образовательной программы _____ К.Б. Сентяков

__03 июня__ 2020 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)».
Трудоемкость (з.е. / часы)	3 з.е. / 108 часов
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 преподавания дисциплины является формирование способности принимать решения в профессиональной области с учетом требований информационной безопасности

Задачи дисциплины: изучение основ информационного законодательства Российской Федерации, правил нормативного регулирования в сфере информационной безопасности, знаний о правонарушениях в информационной сфере

В результате изучения дисциплины студент должен

знать:

- содержание основных понятий по правовому обеспечению информационной безопасности;
- правовых основ защиты государственной тайны и конфиденциальной информации;
- виды ответственности в области правонарушений в информационной сфере

уметь:

- использовать правовые знания в области информационной безопасности в решении профессиональных задач
- участвовать в разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем

владеть:

- навыками применения нормативно правовых актов в области информационной безопасности автоматизированных систем

2. Место дисциплины в структуре ООП:

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

Для изучения дисциплины студент должен

знать:

– основы государства и права;
– основные положения Конституции Российской Федерации;
– федеративное устройство государства и его функции
– системы органов государственной власти
– понятие правонарушения и юридической ответственности, значение законности и правопорядка в современном обществе

уметь:

– уметь правильно толковать законы и иные нормативные правовые акты
– уметь принимать решения и совершать действия в точном соответствии с законом
– уметь ориентироваться в специальной юридической литературе;

владеть:

- навыками работы с нормативно – правовыми документами

Изучение дисциплины базируется на знаниях, полученных при изучении дисциплин: Информатика, Правоведение

Требования к результатам освоения дисциплины

3.1. Знания, приобретаемые в ходе изучения дисциплины

№ п/п З	Знания
1.	Основных понятий по правовому обеспечению информационной безопасности
2.	Правовых основ защиты государственной тайны и конфиденциальной информации
3.	Видов правонарушений и ответственности в области информационной безопасности

3.2. Умения, приобретаемые в ходе изучения дисциплины

№ п/п У	Умения
1.	Использовать правовые знания в области информационной безопасности в решении профессиональных задач
2.	Участвовать в разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем

3.3. Навыки, приобретаемые в ходе изучения дисциплины

№ п/п	Навыки
1.	Применения нормативно правовых актов в области информационной безопасности

3.4.Компетенции, приобретаемые в ходе изучения дисциплины

Компетенции	Индикаторы	Знания (№№ из 3.1)	Умения (№№ из 3.2)	Навыки (№№ из 3.3)
УК-2. Способность 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 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 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	1,2	1
ОПК-3. Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	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 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 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	1,2	1

3. Структура и содержание дисциплины

4.1. Разделы дисциплин и виды занятий

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды контактной работы, самостоятельная работа студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				лек	*прак*	*лаб*	*СРС**	
1	Введение. Основные направления государственной политики в области защиты информации	5	1 2 3	2 2 2	2 2		8	Ответы на вопросы Подготовка к зачету
2	Основные понятия нормативно-правового обеспечения информационной безопасности	5	4 5	2 2			10	Ответы на вопросы Подготовка к зачету
3	Правовые основы защиты государственной и коммерческой тайн.	5	6 7 8	2 2 2	2 2		10	Ответы на вопросы Подготовка к зачету
4	Правовые основы лицензирования и сертификации в области защиты информации	5	9	2	2		8	Ответы на вопросы Подготовка к зачету
5	Правовые основы защиты персональных данных, ГИС (государственных информационных систем), объектов КИИ (критической информационной инфраструктуры)	5	10 11 12 13 14	2 2 2 2 2	 2 2		14	Ответы на вопросы Подготовка к зачету
6	Нормативно – правовое обеспечение в сфере использования криптографических средств защиты информации	5	15 16	2 2	2		8	Ответы на вопросы Подготовка к зачету
							2	Зачет
	Всего	108		**32**	**16**		**60**	
	В том числе контроль самостоятельной работы				2			

4.2. Содержание разделов курса

№ п/п	Раздел Дисциплины	Знания (номер из 3.1)	Умения (номер из 3.2)	Навыки (номер из 3.3)
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.	1,2	1, 2	1
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	1,2,3	1,2	1
3	1. Основные понятия в области защиты	1,2,3	1,2	1

	государственной тайны. 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.			
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	1,2,3	1,2	1
5	1. Законодательство в области защиты персональных данных 2. Классификация информационных систем персональных данных. Базовая и частная модели угроз безопасности 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 РФ	1,2,3	1,2	1
6	1. Нормативно – правовое обеспечение в сфере связи и коммуникации 2. Государственное регулирование вопросов использования криптографических средств и ЭЦП 3. Основы государственного контроля в области защиты информации.	1,2,3	1,2	1

4.3. Наименование тем практических занятий, их содержание и объем в часах

№ п/п	№ раздела дисциплины	Наименование практических работ	Трудоемкость (час)
1.	**1-2**	Анализ терминов и определений информационной безопасности . Национальные интересы РФ в области ИБ, приоритетные направления в области защиты информации. Органы, обеспечивающие национальную безопасность РФ	4
2.	**3**	Законодательство в области защиты государственной тайны. Перечень сведений, отнесенных к государственной тайне. Примеры нормативно -правовых документов в области защиты государственной тайны.	2
3	**3**	Законодательство в области защиты коммерческой тайны. Примеры нормативно правовых актов в области защиты коммерческой тайны.	2
4	**4**	Анализ и подбор сертифицированных средств защиты информации	2
5	**5**	Составления акта классификации информационной системы персональных данных. Классификация ГИС.	2
6	**5**	Анализ законодательства в области защиты КИИ. Категорирование объектов КИИ.	2
7	**6**	Законодательство в области криптографической защиты информации. ГОСТ 28147-89, ГОСТ Р 34.10-2012	2
	Всего		16

4.4.Наименование тем лабораторных работ, их содержание и объем в часах

Лабораторные работы учебным планом не предусмотрены.

4. Содержание самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

5.1. Содержание самостоятельной работы

№ п/п	№ раздела дисциплины	Наименование тем	Трудоем-кость (час)
1.	1-2	Развитие (изменение) информационного законодательства за последние пять лет.	10
2.	3	Понятие коммерческой тайны. Правовое обеспечение защиты коммерческой тайны.	10
3	2	Понятие служебной тайны. Правовое обеспечение защиты служебной тайны.	8
4	4-5	Информационная безопасность государственного и коммерческого предприятия	10
5	5-6	Проекты нормативных документов в области защиты персональных данных; объектов КИИ, криптографической защиты информации	20
6	1-6	зачет	2
	Всего		**60**

5.2. Оценочные средства, используемые для текущего контроля успеваемости и промежуточной аттестации обучающихся по итогам освоения дисциплины, их виды и формы, требования к ним и шкалы оценивания приведены в приложении к рабочей программе дисциплины «Фонд оценочных средств по дисциплине «Правовые основы информационной безопасности», которое оформляется в виде отдельного документа.

5. Учебно-методическое и информационное обеспечение дисциплины:

а) Основная литература

№ п/п	Наименование книги	Год издания
1	Кубанков, А. Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс] : учебное пособие / А. Н. Кубанков, Н. Н. Куняев ; под ред. А. В. Морозов. — Электрон. текстовые данные. — М. : Всероссийский государственный университет юстиции (РПА Минюста России), 2014. — 78 c. — 978-5-89172-850-9. — Режим доступа: http://www.iprbookshop.ru/47262.html	2014
2	Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Электрон. текстовые данные. — М. : ЮНИТИ-ДАНА, 2017. — 287 c. — 978-5-238-02857-6. — Режим доступа: http://www.iprbookshop.ru/72444.html	2017

б) Дополнительная литература

№ п/п	Наименование книги	Год издания
1	Морозов, А. В. Информационное право и информационная безопасность. Часть 2 [Электронный ресурс] : учебник для магистров и аспирантов / А. В. Морозов, Л. В. Филатова, Т. А. Полякова. — Электрон. текстовые данные. — Москва, Саратов : Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. — 604 c. — 978-5-00094-297-0. — Режим доступа: http://www.iprbookshop.ru/66771.html	2016
2	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	2014

в) перечень ресурсов информационно-коммуникационной сети Интернет

1. Электронно-библиотечная система IPRbooks http://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 Web of Science - http://webofscience.com
6. Научная электронная библиотека eLIBRARY.RU – https://elibrary.ru/defaultx.asp

г) программное обеспечение:

1. Microsoft Office Standard 2007
2. Doctor Web Enterprise Suite

д) методические указания:

1. Оформление контрольных работ, рефератов, курсовых работ и проектов, отчетов по практике, выпускных квалификационных работ: методические указания/сост.: А.Ю. Уразбахтина, Р.М. Бакиров, В.А. Смирнов – Воткинск: Изд. ВФ ИжГТУ имени М.Т. Калашникова,2018–25с.- Режимдоступа:http://vfistu.ru/images/files/Docs/metodichka_po_oformleiu_v3.pdf
2. Учебно-методическое пособие по организации самостоятельной работы обучающихся: для обучающихся по направлению подготовки 15.03.05 – конструкторско-технологическое обеспечение машиностроительных производств/ сост.: Р.М. Бакиров, Е.В. Чумакова. – Воткинск: изд. ВФ ИжГТУ имени М.Т. Калашникова,2019–15с.- Режимдоступа:http://vfistu.ru/images/files/Docs/metorg_po_sam_rabote.pdf

7. Материально-техническое обеспечение дисциплины:

1. Специальные помещения - учебные аудитории для проведения занятий лекционного типа, оборудованные доской, столами, стульями.
2. Специальные помещения - учебные аудитории для проведения: занятий семинарского типа, групповых и индивидуальных консультаций, оборудованные доской, столами, стульями.
3. Специальные помещения - учебные аудитории для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся, оборудованные доской, столами, стульями.
4. Специальные помещения - учебные аудитории для организации и проведения самостоятельной работы студентов, оборудованные доской, компьютерами с возможностью подключения к сети «Интернет», столами, стульями.

Лист согласования рабочей программы дисциплины «Правовые основы информационной безопасности» на учебный год

Рабочая программа дисциплины «Правовые основы информационной безопасности» по направлению подготовки 09.03.01 «Информатика и вычислительная техника» по профилю «Автоматизированные системы обработки информации и управления»

согласована на ведение учебного процесса в учебном году:

Учебный год	***«Согласовано»:*** *заведующий кафедрой, ответственной за РПД (подпись и дата)*
2020 – 2021	1.09.20
2021 – 2022	1.09.21
2022 – 2023	
2023 – 2024	

Приложение к рабочей программе дисциплины

МИНОБРНАУКИ РОССИИ
Воткинский филиал
Федерального государственного бюджетного образовательного учреждения высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»
(ВФ ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)

Оценочные средства по дисциплине

Правовые основы информационной безопасности

направление 09.03.01 «Информатика и вычислительная техника»

профиль «Автоматизированные системы обработки информации и управления»

уровень образования: бакалавриат

форма обучения: очная

общая трудоемкость дисциплины составляет: 3 зачетных единиц(ы)

Паспорт
фонда оценочных средств
по дисциплине «Правовые основы информационной безопасности»

(наименование дисциплины)

№ п/п	Раздел Дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Введение. Основные направления государственной политики в области защиты информации	УК-2, ОПК-3	работа на практических занятиях: текущий контроль выполнения заданий; зачет
2	Основные понятия нормативно- правового обеспечения информационной безопасности		работа на практических занятиях: текущий контроль выполнения заданий
3	Правовые основы защиты государственной и коммерческой тайн.		работа на практических занятиях: текущий контроль выполнения заданий
4	Правовые основы лицензирования и сертификации в области защиты информации		работа на практических занятиях: текущий контроль выполнения заданий
5	Правовые основы защиты персональных данных, ГИС (государственных информационных систем), объектов КИИ (критической информационной инфраструктуры)		работа на практических занятиях: текущий контроль выполнения заданий
6	Нормативно – правовое обеспечение в сфере использования криптографических средств защиты информации		работа на практических занятиях: текущий контроль выполнения заданий

Описания элементов ФОС

Наименование: дифференцированный зачет

***Представление в ФОС*:** перечень вопросов

Перечень вопросов для проведения зачета:

1. Определения информационной безопасности. Деятельность по обеспечению информационной безопасности. Методы обеспечения информационной безопасности
2. Уровни правового обеспечения информационной безопасности. Примеры НПА различного уровня в области защиты информации
3. Категории информации по условиям доступа к ней. Информация как объект правовых отношений.
4. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и его краткая характеристика.
5. Понятия «доктрина», «концепция», «стратегия», их общая характеристика на примере применения в Российской Федерации.
6. Доктрина информационной безопасности Российской Федерации от 05.12.2016г. и ее краткая характеристика
7. Государственная программа Российской Федерации " О стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" (Указ Президента РФ №7668 от 09 мая 2017) и ее краткая характеристика
8. Роль и место организационной защиты в структуре мер по защите информации. Основные принципы организационной защиты информации.
9. Принципы (правила) организационной системы защиты информации.
10. Организационные мероприятия по обеспечению информационной безопасности
11. Федеральный закон «О коммерческой тайне» и его краткая характеристика
12. Принципы отнесение информации к коммерческой тайне
13. Закон РФ от 21 июля 1993 г. № 5485-I «О государственной тайне» и его краткая характеристика
14. Принципы отнесение информации к гостайне. Грифы секретности информации, относящейся к гостайне и коммерческой информации
15. Организационная структура системы обеспечения информационной безопасности

Российской Федерации

16. Структуру органов исполнительной власти Удмуртской Республики; органы исполнительной власти, непосредственно отвечающие за информационное обеспечение
17. Федеральная служба по техническому и экспортному контролю (ФСТЭК России), ее функции и полномочия в информационной сфере.
18. Сертификация программно-аппаратных средств по требованиям информационной безопасности
19. Федеральная служба безопасности Российской Федерации, ее функции и полномочия в информационной сфере.
20. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и его краткая характеристика.
21. Обзор основных нормативно - правовых актов в области защиты персональных данных.
22. Классификация информационных систем персональных данных
23. Нормативная база в области защиты и классификация государственных информационных систем.
24. Нормативная база в области защиты объектов ключевой критической инфраструктуры
25. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и его краткая характеристика.
26. Статья 272 УК РФ (Неправомерный доступ к компьютерной информации). Рассмотреть по составу.
27. Статья 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ). Рассмотреть по составу.
28. Статья 274 УК РФ (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей). Рассмотреть по составу.
29. Статья 183 УК РФ (Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну).
30. Статья 13.12 КоАП РФ. Нарушение правил защиты информации
31. Статья 13.13 КоАП РФ. Незаконная деятельность в области защиты информации
32. Статья 13.14 КоАП РФ. Разглашение информации с ограниченным доступом

Критерии оценки:
приведены в разделе 2

Наименование: работа на практических занятиях: текущий контроль выполнения заданий.
***Представление в ФОС*:** перечень заданий
Варианты заданий:

- Дайте определение термину "информационная безопасность"
- Проанализируйте основные положения ФЗ-149 "Об информации, информационных технологиях и защите информации"
- Перечислите законодательство в области защиты персональных данных
- Дайте определение и приведите примеры "Объектов критической инфраструктуры"
- Опишите роль следующих организаций в области ЗИ: ФСТЭК, ФСБ, АНБ
- Найти и проанализировать методические документы на сайте регулятора ИБ www.fstec.ru.
-

Критерии оценки:
Приведены в разделе 2

2 Критерии оценки:

Уровень освоения компетенции						
	Компетенции	**Дескрипторы**	**Вид, форма оценочного мероприятия**	**Компетенция освоена***		
				отлично	**хорошо**	**удовлетворительно**	**неудовлетворительно**
	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	З1- Основных понятий по правовому обеспечению информационной безопасности З2- Правовых основ защиты государственной тайны и конфиденциальной информации З3- Видов правонарушений и ответственности в области информационной безопасности	Диф. зачет	заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание учебного материала, предусмотренного программой, усвоивший основную литературу и знакомый с дополнительной литературой, рекомендованной программой.	заслуживает обучающийся, обнаруживший полное знание учебного материала, усвоивший основную литературу, рекомендованную в программе. Оценка "хорошо" выставляется обучающимся, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	заслуживает обучающийся, обнаруживший знания основного учебного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, знакомых с основной литературой, рекомендованной программой. Оценка выставляется обучающимся, допустившим погрешности в ответе на зачете и при выполнении заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя.	выставляется обучающемуся, обнаружившему пробелы в знаниях основного учебного материала. Оценка ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании образовательного учреждения без дополнительных занятий по рассматриваемой дисциплине

	основных требований информационной безопасности;	У1 - Использовать правовые знания в области информационной безопасности в решении профессиональных задач У2 -Участвовать в разработке документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем Н1 - Применения нормативно правовых актов в области информационной безопасности	Работа на практических занятиях: текущий контроль выполнения заданий	Правильно выполнены все задания. Продемонстрирован высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	Правильно выполнена большая часть заданий. Присутствуют незначительные ошибки. Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий	Задания выполнены более чем наполовину. Присутствуют серьёзные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие Способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены менее чем наполовину. Продемонстрирован неудовлетворительный уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению