УТВЕРЖДАЮ
Проректор по учебной работе
_________ / В.Е. Федоров
«25» июня 2021 г.

Рабочая программа дисциплины (модуля)*

Организационное и правовое обеспечение информационной безопасности

Направление подготовки (специальность)

10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль)

специализация № 4 «Безопасность автоматизированных систем критически важных объектов»

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год набора 2021

*Рабочая программа дисциплины (модуля) адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

Челябинск 2021 г.

Рабочая программа дисциплины (модуля) принята:

Ученым советом Физического факультета

Протокол заседания № «13» от 24.05 2021 г.

Председатель Ученого совета Физического факультета _____ Ф.А. Захарьевич

Секретарь Ученого совета Физического факультета _____ И.А. Эбель

Рабочая программа дисциплины (модуля) одобрена и рекомендована кафедрой

Прокурорского надзора и организации правоохранительной деятельности

Протокол заседания №10 от 24 мая 2021г.

Заведующий кафедрой _____ А.В. Майоров

Авторы (составители) _____ к.ю.н., зав.кафедрой А.В.Майоров

_____ ст. преподаватель, Т.П. Макашова

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 274-1

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Преподавание учебной дисциплины «Организационное и правовое обеспечение информационной безопасности» носит теоретико-прикладной характер и предполагает ознакомление студентов с нормативными правовыми актами и стандартами в области защиты информации, а также основами организационного и технического обеспечения защиты информации, с учетом практики применения и достижений правовой науки. Направлено на формирование у студентов практических навыков работы в реальных конкретных условиях.

Цель обучения состоит в формировании научно-обоснованного представления об основах организационной защиты информации в Российской Федерации и ее значения в деятельности правоохранительных органов власти и других организаций. Курс посвящен изучению современного представления о методах и средствах организационного обеспечения защиты информационных ресурсов, а также информационной безопасности личности, общества и государства.

Задачи обучения:

- изучение теоретических, методологических и практических проблем формирования, функционирования и развития систем организационной защиты информации;

- ознакомление с понятийным аппаратом в области организационной защиты информации;

- рассмотрение базовых содержательных положений в области организационной защиты информации;

- определение целей и принципов организационной защиты информации;

- ознакомление с составом организационной защиты информации, ее компонентами;

- установление структуры организационной защиты информации;

- ознакомление с процессами планирования в организационной защиты информации;

- рассмотрение методов и особенностей применяемых в организационной защите информации в зависимости от характера защищаемой информации;

- определение назначения, сущности и структуры системы организационной защиты информации.

Индикаторы достижения компетенций:

УК-2.1. Определяет этапы жизненного цикла проекта и выстраивает последовательность их реализации.

УК-2.2. Формулирует проблему, на решение которой направлен проект, грамотно определяет цель проекта.

УК-2.3. Проектирует решение конкретных задач проекта, выбирая оптимальный способ их решения.

ОПК-5.1. Обладает знаниями о нормативных правовых актах, нормативных и методических документах, регламентирующих деятельность по защите информации.

ОПК-5.2. Демонстрирует умения применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	К.М.02.09

2.1 Требования к предварительной подготовке обучающегося:

Техническая защита информации

Основы информационной безопасности

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Разработка модели угроз безопасности информации в автоматизированных системах

Обеспечение информационной безопасности на критически важных объектах

Защита информации от утечки по техническим каналам

Методы и средства противодействия террористической деятельности в системах управления критически важных объектов

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

УК-2: Способен управлять проектом на всех этапах его жизненного цикла

Знать:

Для достижения индикатора УК-2.1: Знать этапы жизненного цикла проекта и последовательность их реализации.

Уметь:

Для достижения индикатора УК-2.2: Уметь формулировать проблему, на решение которой направлен проект, грамотно определять цель проекта.

Владеть:

Для достижения индикатора УК-2.3: Владеть навыками проектирования решения конкретных задач проекта, выбирая оптимальный способ их решения.

ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

Знать:

Для достижения индикатора ОПК-5.1: Знать источники и классификацию угроз информационной безопасности, требования по защите информации при использовании СКЗИ, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.

Уметь:

Для достижения индикатора ОПК-5.2: Уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности, классифицировать и оценивать угрозы информационной безопасности для объекта информатизации, разрабатывать требования к системе защиты информации.

Владеть:

Для достижения индикатора ОПК-5.2: Владеть навыками работы с нормативными правовыми актами в области информационной безопасности, применения современной нормативной базы для построения системы организационных и программно-технических мер по выявлению и нейтрализации угроз безопасности компьютерных систем.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	этапы жизненного цикла проекта и последовательность их реализации;
3.1.2	источники и классификацию угроз информационной безопасности;
3.1.3	требования по защите информации при использовании СКЗИ;
3.1.4	основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.
3.2	**Уметь:**
3.2.1	формулировать проблему, на решение которой направлен проект, грамотно определять цель проекта;
3.2.2	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
3.2.3	классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
3.2.4	разрабатывать требования к системе защиты информации.
3.3	**Владеть:**
3.3.1	навыками проектирования решения конкретных задач проекта, выбирая оптимальный способ их решения;
3.3.2	навыками работы с нормативными правовыми актами в области информационной безопасности;
3.3.3	навыками применения современной нормативной базы для построения системы организационных и программно-технических мер по выявлению и нейтрализации угроз безопасности компьютерных систем.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)	
Общая трудоемкость	**3 ЗЕТ**
Часов по учебному плану: 108 в том числе: аудиторные занятия: 72 самостоятельная работа: 36	Виды контроля в семестрах: зачеты 8

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Тема 1. Информация как объект правового регулирования			

1.1	Информация как объект правового регулирования /Лек/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
1.2	Информация как объект правового регулирования /Пр/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
1.3	Информация как объект правового регулирования /Ср/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
	Раздел 2. Тема 2. Правые вопросы обеспечение информационной безопасности			
2.1	Правые вопросы обеспечение информационной безопасности /Лек/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
2.2	Правые вопросы обеспечение информационной безопасности /Пр/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
2.3	Правые вопросы обеспечение информационной безопасности /Ср/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
	Раздел 3. Тема 3. Правовое регулирование отношений по защите государственной тайны			
3.1	Правовое регулирование отношений по защите государственной тайны /Лек/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
3.2	Правовое регулирование отношений по защите государственной тайны /Пр/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
3.3	Правовое регулирование отношений по защите государственной тайны /Ср/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
	Раздел 4. Тема 4. Правовое регулирование отношений, связанных с режимом коммерческой тайны			

4.1	Правовое регулирование отношений, связанных с режимом коммерческой тайны /Лек/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
4.2	Правовое регулирование отношений, связанных с режимом коммерческой тайны /Пр/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
4.3	Правовое регулирование отношений, связанных с режимом коммерческой тайны /Ср/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
	Раздел 5. Тема 5. Правовое регулирование отношений в области обработки персональных данных			
5.1	Правовое регулирование отношений в области обработки персональных данных /Лек/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
5.2	Правовое регулирование отношений в области обработки персональных данных /Пр/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
5.3	Правовое регулирование отношений в области обработки персональных данных /Ср/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
	Раздел 6. Тема 6. Правовое регулирование электронного документооборота			
6.1	Правовое регулирование электронного документооборота /Лек/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
6.2	Правовое регулирование электронного документооборота /Пр/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
6.3	Правовое регулирование электронного документооборота /Ср/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
	Раздел 7. Тема 7. Правовое регулирование отношений в области связи и массовых коммуникаций			

7.1	Правовое регулирование отношений в области связи и массовых коммуникаций /Лек/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
7.2	Правовое регулирование отношений в области связи и массовых коммуникаций /Пр/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
7.3	Правовое регулирование отношений в области связи и массовых коммуникаций /Ср/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
	Раздел 8. Тема 8. Правовое регулирование отношений в области библиотечного и архивного дела			
8.1	Правовое регулирование отношений в области библиотечного и архивного дела /Лек/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
8.2	Правовое регулирование отношений в области библиотечного и архивного дела /Пр/	8	4	Л2.1 Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
8.3	Правовое регулирование отношений в области библиотечного и архивного дела /Ср/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
	Раздел 9. Тема 9. Правовое регулирование отношений в сфере организации и деятельности средств массовой информации			
9.1	Правовое регулирование отношений в сфере организации и деятельности средств массовой информации /Лек/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
9.2	Правовое регулирование отношений в сфере организации и деятельности средств массовой информации /Пр/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5
9.3	Правовое регулирование отношений в сфере организации и деятельности средств массовой информации /Ср/	8	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3 Э4 Э5

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Доклад
тест
зачет

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Примерные тесты для текущего контроля знаний:
1. К основным организационным мероприятиям по защите информации можно отнести:
а) организацию режима и охраны; организацию работы с сотрудниками; организацию работы с документами; организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации; организацию работы по анализу внутренних и внешних угроз конфиденциальной информации; организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией.
б) организацию охраны подвижных объектов; организацию работы с партнерами; организацию работы с документами; организацию контрразведывательных мероприятий; организацию работы по анализу внутренних и внешних угроз конфиденциальной информации; организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией
в) организацию пропускного режима; организацию работы с клиентами; организацию использования технических средств сбора и хранения конфи¬денциальной информации; организацию аналитической работы.
2. Силы и средства защиты коммерческого предприятия в зависимости от решаемых задач, условий, специфических особенностей подразделяются на следующие основные направления защиты:
а) правовой защиты, технической защиты, специальной защиты, информационно-коммерческой защиты.
б) правовой защиты, инженерно-технической защиты, организационной защиты.
в) физической защиты, технической защиты, специальной защиты, морально-психологической защиты.
3. Под политикой информационной безопасности понимается:
а) разработка пакета документов, направленных на защиту информации и ассоциированных с ней ресурсов.
б) отдача указаний и контроль за их выполнением, направленных на защиту информации и ассоциированных с ней ресурсов.
в) совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.
4. Основными задачами сил и средств физического защиты фирмы являются:
а) - организация личной охраны руководителей фирмы и ведущих специалистов.
- организация охраны персонала и аттестованных по режиму конфиденциальных помещений.
- организация и поддержание пропускного и внутри объектового режима.
- организация и установление мер физической и технической защиты зданий и помещений.
- организация и осуществление мер по обеспечению безопасности деятельности и защиты сведений, составляющих государственную и коммерческую тайну.
- разработка и совершенствование системы предотвращения несанкционированного доступа и допуска к сведениям, составляющим коммерческую тайну.
- организация, разработка и контроль системы безопасности в повседневных и особых условиях.
б) - организация личной охраны всего персонала предприятия.
- организация внутри объектового режима.
- организация и установление мер физической и технической защиты при перевозке ценных грузов.
- организация и осуществление мер защите сведений, составляющих коммерческую тайну.
- разработка системы предотвращения несанкционированного доступа к сведениям, составляющим коммерческую тайну.
в) - организация личной охраны администрации фирмы и членов их семей.
- организация охраны стационарных объектов предприятия.
- осуществление мер по защите сведений, составляющих государственную тайну.
- разработка системы предотвращения несанкционированного доступа к сведениям, составляющим коммерческую тайну.
- организация, разработка и контроль системы безопасности в особых условиях.
5. К основным техническим средствам безопасности коммерческого предприятия относятся:
а) средства физической защиты, аппаратные средства защиты, программные средства защиты, правовые методы защиты.
б) средства физической защиты, аппаратные средства защиты, программные средства защиты, математические (криптографические) методы защиты
в) средства физической защиты, производственные средства защиты, информационно-коммерческие методы защиты
6. Основными принципами создания и поддержания организационного обеспечения комплексной безопасности являются:
а) законности, комплексности, обоснованности, соблюдение баланса защиты жизненно важных интересов предприятия и субъекта защиты, ответственности за порученный участок работы, децентрализации управления.
б) законности, плановости, обособленности, соблюдение баланса защиты жизненно важных интересов предприятия и государства, непрерывности, централизации управления, взаимодействия и координации
в) законности, комплексности, обоснованности, соблюдение баланса защиты жизненно важных интересов предприятия и субъекта защиты, взаимной ответственности, централизации управления, взаимодействия и координации.

7. Система безопасности предприятия действует на основе следующих организационно-правовых документов:
а) Конституции РФ. Устава области. Федерального закона «О безопасности».
б) Устава. Положения о системе собственной безопасности. Руководства по защите конфиденциальной информации. Инструкции о порядке работы с иностранными специалистами. Руководства по инженерно-технической защите помещений и технических средств.
в) Конвенции по правам человека. Положения о системе коллективной безопасности. Приказов и инструкций по безопасности.
8. Внешний контроль над деятельностью службы безопасности осуществляют:
а) органы внутренних дел; следственные органы; прокуратура; суд; общественные организации.
б) органы внутренних дел; следственные органы; прокуратура; суд; политические партии и движения
в) органы внутренних дел; следственные органы; прокуратура; суд; другие административные органы по вопросам, отнесенным к их компетенции в сфере частной детективной и охранной деятельности.
9. В целях сыска служба безопасности имеет право:
а) проводить допрос граждан и должностных лиц. Наводить справки. Изучать предметы и документы. Вести розыск утраченного (похищенного) иму¬щества. Вести негласное наблюдение и прослушивание граждан. Приобретать, хранить и применять в установленном порядке огнестрельное оружие. Оказывать содействие правоохранительным органам в обеспечении правопорядка, в том числе и на договорной основе.
б) проводить устный опрос граждан и должностных лиц. Изучать предметы и документы. Вести розыск похищенного имущества. Вести наблюдение. Применять в установленном порядке специальные средства.
в) проводить устный опрос граждан и должностных лиц (с их согласия). Наводить справки. Изучать предметы и документы (с письменного согласия их владельцев). Вести розыск утраченного (похищенного) имущества. Вести наблюдение. Использовать видео-, аудиозаписи, кино- и фотосъемки (в порядке, установленном законом), технические и иные средства, не причиняющие вреда жизни и здоровью граждан и окружающей среде, а также средства оперативной радио- и телефонной связи. Приобретать, хранить и применять в установленном порядке специальные средства. Оказывать содействие правоохранительным органам в обеспечении правопорядка, в том числе и на договорной основе.
10. По отношению к информации и информационным ресурсам проявляются следующие угрозы:
а) целостности; подделке; полноты; доступности.
б) целостности; конфиденциальности; фальсификации; доступности.
в) целостности; конфиденциальности; полноты; доступности.
11. Существует следующие формы допуска к секретным работам и документам:
а) - наивысшая форма допуска (имеют право на ознакомление со сведениями «особой важности», «совершенно секретно», «секретно»).
- вторая форма допуска (имеют право на ознакомление со сведениями «совершенно секретно», «секретно»).
- третья форма допуска (имеют право на ознакомление со сведениями «секретно»).
б) - наивысшая форма допуска (имеют право на ознакомление со сведениями «особой важности», «совершенно секретно», «секретно»).
- вторая форма допуска (имеют право на ознакомление со сведениями «совершенно секретно», «секретно»).
- третья форма допуска (имеют право на ознакомление со сведениями «секретно» и «для служебного пользования»).
в) - наивысшая форма допуска (имеют право на ознакомление со сведениями «особой важности»).
- вторая форма допуска (имеют право на ознакомление со сведениями «совершенно секретно»). Третья форма допуска (имеют право на ознакомление со сведениями «секретно»).
12. Условия прекращения допуска должностного лица или гражданина к государственной тайне:
а) расторжения с ним трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий; длительным отсутствием на рабочем месте (например по болезни); возникновения обстоятельств, являющихся согласно статье 22 Закона «О государственной тайне» основанием для отказа должностному лицу или гражданину в допуске к государственной тайне.
б) расторжения с ним трудового договора (контракта) в связи с про¬ведением организационных и (или) штатных мероприятий; однократного нарушения им взятых на себя предусмотренных трудовым договором (контрактом) обязательств, связанных с защи¬той государственной тайны; возникновения обстоятельств, являющихся согласно статье 22 Закона «О государственной тайне» основанием для отказа должностному лицу или гражданину в допуске к государственной тайне.
в) в связи с переходом на новую должность; однократного нарушения им взятых на себя предусмотренных трудовым договором (контрактом) обязательств, связанных с защитой государственной тайны; в связи с увольнением из предприятия.
13. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне могут касаться:
а) права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне; права на хранение сведений, составляющих государственную тайну; права на проведении проверочных мероприятий в период нахождения в отпуску.
б) права выезда за город, на дачу без охраны на срок; права на продажу сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения; права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.

в) права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне; права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения; права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.

14. Допуск специалиста к коммерческим секретам обязывает:

а) строго соблюдать требования инструкций по работе с коммерческими секретами; ответственность за нарушение режима информационной безопасности.

б) строго соблюдать требования руководства предприятия по вопросам трудового договора; обязательства по предоставлению гарантий и компенсаций за работу с конфиденциальной информацией.

в) быстрый карьерный рост по работе; применять свои права в области соблюдения режима информационной безопасности.

15. Под режимом КТ следует понимать:

а) выполнение обладателем информации, состав¬ляющей КТ, неукоснительное исполнение распоряжений руководства по охране ее конфиденциальности коммерческих секретов.

б) проведение руководством предприятия комплекса мер по расследованию нарушений обращения с конфиденциальной информацией

в) правовые, организационные, технические и иные принимаемые обладателем информации, составляющей КТ, меры по охране ее конфиденциальности.

16. Обладатель информации, составляющей государственную тайну, имеет право:

а) использовать информацию, составляющую государственную тайну, для собственных нужд.

б) по своему усмотрению передавать секретную информацию сторонним организациям.

в) вносить предложения по вопросам совершенствования режима охраны государственной тайны.

17. Комиссия, проводящая служебное расследование по факту нарушения информационной безопасности, обязана:

а) - установить условия, обстоятельства и причины разглашения сведений или утраты документов и выработать рекомендации по их устранению;

- использовать все имеющиеся возможности по розыску утраченного документа;

- выявить лиц, виновных в разглашении сведений или утрате документа.

б) - установить условия, обстоятельства и причины разглашения сведений или утраты документов и выработать рекомендации по их устранению;

- использовать все имеющиеся возможности для передачи дела в суд;

- выявить лиц, виновных в разглашении сведений или утрате документа.

в) - оповестить руководство предприятия о нарушении информационной безопасности;

- использовать все имеющиеся возможности по розыску утраченного документа;

- выявить лиц, виновных в разглашении сведений или утрате документа.

18. Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие льготы:

а) - процентные надбавки к заработной плате в зависимости от сте¬пени секретности сведений, к которым они имеют доступ;

- быстрый карьерный рост.

б) - процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;

- преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий.

в) - процентные надбавки к заработной плате в зависимости от сте¬пени секретности сведений, к которым они имеют доступ;

- моральное стимулирование.

19. Основаниям для отказа должностному лицу или гражданину в допуске к государственной тайне могут являться:

а) постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства;

б) постоянное проживание его близких родственников в другом регионе страны;

в) временное проживание его самого на съемных квартирах или в гостиницах.

20. Эффективная защита обеспечивается при выполнении следующих условий:

а) - единство в решении производственных, коммерческих, финансовых и режимных вопросов;

- координация мер безопасности между заинтересованными подразделениями фирмы;

- разработка режимных мер на основе оценки информации и объектов, подлежащих защите (классификации);

- персональная ответственность на всех исполнительских уровнях за обеспечение сохранности конфиденциальной информации;

- централизацией специального делопроизводства;

- наличием списка лиц, допущенным к такого рода информации;

- наличие вооруженной охраны, а также введением усиленных пропускных режимов.

б) - единство в решении производственных, коммерческих, финансовых и режимных вопросов;

- координация мер безопасности между заинтересованными подразделениями фирмы;

- разработка режимных мер на основе оценки информации и объектов, подлежащих защите (классификации);

- персональная ответственность на всех исполнительских уровнях за обеспечение сохранности конфиденциальной информации;
- организация специального делопроизводства, введение соответствующей маркировки документов;
- разработка и утверждение списка с перечнем лиц, допущенным к такого рода информации;
- наличие охраны, а также пропускного и внутриобъектового режимов.

в) - единство в решении производственных, коммерческих, финансовых и режимных вопросов;
- координация мер безопасности между заинтересованными подразделениями фирмы;
- разработка режимных мер на основе оценки информации и объектов, подлежащих защите (классификации);
- персональная ответственность на всех исполнительских уровнях за обеспечение сохранности конфиденциальной информации;
- организация специального делопроизводства, введение соответствующей маркировки документов;
- разработка и утверждение списка с перечнем лиц, допущенным к такого рода информации;
- наличием вневедомственной охраны.

21. Объектами охраны предприятия выступают:

а) Стационарные объекты. Руководство предприятия и их семьи. Денежные средства. Ценные бумаги и другие ценности.

б) Стационарные объекты. Подвижные объекты. Персонал. Денежные средства. Ценные бумаги и другие ценности.

в) Стационарные объекты. Отдельные сотрудники предприятия. Денежные средства. Служба безопасности предприятия.

22. Существует несколько видов охраны, в том числе:

а) охрана с помощью привлечения собак (кинологическая служба); охрана путем выставления постов; комбинированная охрана.

б) охрана с помощью технических средств с подключением на пульт централизованного наблюдения и остановкой автоматической сигнализации; охрана путем выставления постов; комбинированная охрана.

в) автономная охрана с помощью технических средств наблюдения и автоматической сигнализации; охрана путем выставления подвижных; комбинированная охрана.

23. Система обеспечения безопасности объекта охранной деятельности должна строиться на следующих принципах:

а) Комплексность. Эшелонирование. Равнопрочность. Разумная достаточность. Непрерывность.

б) Комплексность. Эшелонирование. Оснащенность. Разумная достаточность. Непрерывность.

в) Комплексность. Эшелонирование. Своевременность. Разумная достаточность. Непрерывность.

24. К основным требованиям внутриобъектового режима относится:

а) Соблюдение распорядка рабочего времени. Строгое соблюдение сотрудниками правил производственной безопасности. Установление порядка приема и работы с посетителями сторонних организаций. Порядок сдачи и приема конфиденциальных документов. Порядок ведения факсовых и телекоммуникационных обменов информацией.

б) Установление четкого распорядка рабочего времени. Строгое соблюдение сотрудниками правил взаимоотношений в коллективе. Установление порядка работы с партнерами. Оснащение фирмы техническими средствами обеспечения производственной деятельности. Порядок посещения помещений сотрудниками и посетителями. Порядок ведения телефонных, разговоров.

в) Установление четкого распорядка рабочего времени. Строгое соблюдение сотрудниками правил экономической и информационной безопасности, правил противопожарной и противоаварийной безопасности и техники безопасности. Установление порядка приема и работы с посетителями сторонних организаций. Оборудование фирмы техническими средствами обеспечения производственной деятельности. Порядок сдачи и приема помещений под охрану. Порядок ведения телефонных, факсовых и телекоммуникационных обменов информацией с соблюдением режима конфиденциальности и экономии.

25. По уровню охраны и объему предпринимаемых мер безопасности коммерческие предприятия (организации) подразделяют следующие основные категории:

а) объекты со свободным допуском персонала и клиентов; объекты с простыми ограничениями и ограждениями типа неохраняемых заграждений; объекты с охраняемыми заграждениями, контролируемыми охранниками, с постовыми нарядами, патрульными службами и сотрудниками пропускной системы; объекты с особым режимом охраны, допуск на которые обеспечивается специально подготовленными и расставленными по территории и периферии охранниками и сложными техническими системами с телемониторами и звуковой сигнализацией.

б) объекты со свободным допуском персонала и клиентов; объекты с простыми ограничениями; объекты с особым режимом охраны, допуск на которые обеспечивается охранниками и сложными техническими системами с телемониторами и звуковой сигнализацией.

в) объекты со свободным допуском персонала и клиентов; объекты контролируемыми не вооруженными охранниками службы безопасности предприятия; объекты с усиленным режимом охраны.

Примерные темы докладов:

1. Понятие информации и смежные с ним понятия.
2. Понятие правового режима информации и его разновидности.
3. Информационная политика государства.
4. Сущность права на информационную безопасность и его гарантии.
5. Система законодательства об информационной безопасности.

6. Понятие и правовая природа информационного общества.
7. Обеспечение информационной безопасности личности.
8. Обеспечение информационной безопасности государства.
9. Объективная и субъективная стороны информационной безопасности.
10. Правоотношения в сфере информационной безопасности (понятие, виды, элементы).
11. Правонарушения в информационной сфере: понятие, виды, состав.
12. Гражданско-правовая ответственность за правонарушения в информационной сфере.
13. Административно-правовая ответственность за правонарушения в информационной сфере.
14. Уголовная ответственность за преступления в информационной сфере.
15. Киберпреступления: понятие, основные черты и формы проявления.
16. Принципы формирования сведений, составляющих государственную тайну.
17. Соотношение государственной и служебной тайн.
18. Правовое регулирование международного информационного обмена.
19. Соотношение служебной и коммерческой тайн.
20. Правовое регулирование использования аналогов собственноручной подписи.
21. Правовой режим коммерческой тайны.
22. Правовой режим персональных данных.
23. Правовая защита информации.
24. Право граждан на доступ к информации.
25. Право юридических лиц на получение информации.
26. Информационная открытость органов государственной власти.
27. Информационное обеспечение деятельности органов государственной власти.
28. Правовой режим информации, составляющей государственную тайну.
29. Информационное обеспечение деятельности правоохранительных органов.
30. Особенности правового регулирования отношений в Интернете.
31. Свобода массовой информации: понятие, правовая характеристика.
32. Средства массовой информации как объект права и юридическая фикция.
33. Информация о частной жизни лица: правовое регулирование.
34. Персональные данные как особый институт охраны прав на неприкосновенность частной жизни.
35. Российское законодательство о средствах массовой информации: история развития и общий обзор.
36. Право и Интернет как социальные явления.
37. Источники интернет-права.
38. Правовое регулирование общественных отношений в области архивного дела и архивов.
39. Правовое регулирование общественных отношений в области формирования обязательного экземпляра документов.
40. Порядок распоряжения сведениями, составляющими государственную тайну.
41. Распоряжение исключительным правом на секреты производства.
42. Порядок отнесение информации к секретам производства.
43. Функциональные составляющие коммерческой тайны.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Вопросы к зачету:
1. Организационные источники и каналы утечки.
2. Силы, средства и условия организационной защиты информации
3. Особенности системы организационной защиты информации, составляющей государственную тайну.
4. Особенности системы организационной защиты информации, составляющей служебную тайну.
5. Порядок засекречивания конфиденциальных сведений, документов и изделий.
6. Порядок рассекречивания конфиденциальных сведений, документов и изделий.
7. Особенности подбора сотрудников на должности, связанные с работой с конфиденциальной информацией.
8. Состав документов, необходимых при подборе и приеме сотрудников на должности, связанные с доступом к конфиденциальной информации и особенности документирования трудовых отношений.
9. Понятие и виды ответственности за преступления и правонарушения в сфере защиты информации.
10. Процедура оформления, изменения формы допуска и переоформления допусков и ее документирование.
11. Организация доступа к конфиденциальной информации.
12. Понятие, цели, задачи и основные требования разрешительной системы доступа, предъявляемые к ней.
13. Особенности доступа к конфиденциальной информации различных категорий сотрудников. Обязанности лиц, допущенных к защищаемым сведениям.
14. Мотивация персонала к выполнению требований по защите информации. Основные формы воздействия на персонал как методы мотивации.
15. Организация контроля за соблюдением сотрудников требований режима защиты информации. Методы проверки сотрудников.
16. Основные меры по защите информации при увольнении сотрудника. Документирование процедуры увольнения сотрудника.
17. Организация служебного расследования по фактам разглашения и утечки конфиденциальной информации
18. Организация охраны территории, зданий, помещений и персонала

19. Виды и способы охраны. Факторы выбора приемов и средств охраны.
20. Организация пропускного режимов
21. Организация внутриобъектового режимов
22. Понятие режимных помещений и требования, предъявляемые к ним.
23. Порядок аттестации помещений на пригодность их для ведения конфиденциальных работ и его документальное оформление.
24. Ограничение прав граждан в связи с оформлением допуска к государственной тайне.
25. Понятие, цели, задачи и методики аналитической работы по защите информации.
26. Технология аналитической работы, ее основные этапы.
27. Методы сбора (получения) и оценки информации. Определение состава собираемых данных.
28. Основные методы анализа. Представление и оформление полученных результатов.
29. Планирование процессов организационной защиты информации
30. Информационное общество: понятие, структура, признаки.
31. Понятие информационной сферы общества.
32. Сущность конституционного права на информацию и его гарантии.
33. Правовые режимы информации.
34. Понятие и виды информационных правоотношений.
35. Субъекты, объекты, содержание информационных правоотношений.
36. Законодательство Российской Федерации в области информационной безопасности.
37. Понятие информационной безопасности.
38. Особенности обеспечения информационной безопасности в различных сферах общественной жизни.
39. Понятие правонарушений в информационной сфере.
40. Ответственность за правонарушения в информационной сфере.
41. Понятие государственной тайны. Сведения, составляющие государственную тайну.
42. Отнесение сведений к государственной тайне, их засекречивание и рассекречивание.
43. Порядок распоряжения сведениями, составляющими государственную тайну.
44. Защита сведений, составляющих государственную тайну.
45. Юридическая ответственность за нарушение режима государственной тайны.
46. Понятие коммерческой тайны. Информация, составляющая коммерческую тайну (секреты производства).
47. Отнесение информации к информации, составляющей коммерческую тайну (секрет производства).
48. Содержание и реализация исключительного права на секрет производства.
49. Ответственность за нарушение исключительного права на секрет производства.
50. Понятие и виды персональных данных.
51. Принципы обработки персональных данных.
52. Порядок и условия обработки персональных данных.
53. Права и обязанности субъекта персональных данных.
54. Права и обязанности оператора при обработке персональных данных.
55. Контроль и надзор за обработкой персональных данных.
56. Ответственность за нарушение положений законодательства о персональных данных.
57. Понятие электронного документа и электронного документооборота.
58. Правовое регулирование и юридические риски электронного документооборота.
59. Понятие и виды электронной подписи.
60. Правовой статус удостоверяющего центра.
61. Правовое регулирование отношений в области формирования обязательного экземпляра документов.
62. Правовое регулирование общественных отношений в сфере формирования, хранения, учета и использования архивов и архивных фондов.
63. Понятие связи, ее структура, принципы функционирования.
64. Общая характеристика отношений в сфере связи и массовых коммуникаций.
65. Государственной регулирование деятельности в области связи.
66. Право и Интернет как социальные явления.
67. Особенности регулирования интернет-отношений.
68. Правовое регулирование деятельности в киберпространстве.
69. Киберпреступления: понятие, основные черты, формы проявления.
70. Понятие и распространение массовой информации.
71. Понятие и правовой статус средства массовой информации.
72. Правовые формы организации деятельности средств массовой информации.
73. Общие принципы работы средств массовой информации.
74. Правовые формы организации деятельности средств массовой информации

6.4. Критерии оценивания

Собеседование:
Основной формой проверки знаний и умений студентов по дисциплине «Организационное и правовое обеспечение информационной безопасности» является собеседование (устный опрос в форме зачёта).
Критериями устного ответа выступают следующие качества знаний:
полнота – количество знаний об изучаемом объекте, входящих в программу;

глубина – совокупность осознанных знаний об объекте;
конкретность – умение раскрыть конкретные проявления обобщённых знаний (доказать на примерах основные положения);
системность – представление знаний об объекте в системе, с выделением структурных её элементов, расположенных в логической последовательности;
развёрнутость – способность развернуть знания в ряд последовательных шагов;
осознанность – понимание связей между знаниями, умение выделить существенные и несущественные связи, познание способов и принципов получения знаний.
Ответы студента по вопросам курса «Организационное и правовое обеспечение информационной безопасности» оцениваются по системе « зачтено» / « не зачтено».
Отметка «зачтено» ставится студенту, усвоившему учебный материал в соответствии с программой курса, овладевшему основными понятиями и категориями, ориентирующемуся в учебной литературе, нормативном материале и юридической практике, умеющему использовать нормативный материал для обоснования выводов.
Отметка «не зачтено» ставится студенту, который не знает значительной части учебного материала, не может сформулировать определения понятий, не ориентируется в нормативном материале.

Тест: описание показателей и критериев оценивания компетенций
Оценка Неудовлетворительно Удовлетворительно Хорошо Отлично
Набранная сумма баллов (% выполненных заданий) (мах – 100) Менее 60 60-75 76-85 86-100
Оценка Не зачтено Зачтено
Набранная сумма баллов (% выполненных заданий) (мах – 100) Менее 60 60-100

Доклад: описание показателей и критериев оценивания компетенций
Оценка Не зачтено Зачтено
Оцениваются навыки и умения работы с различным источниками информации, информационными ресурсами и технологиями
знания требований нормативных правовых актов в области информационной безопасности Обучающийся продемонстрировал не знание работы с различным источниками информации, информационными ресурсами и технологиями,
не освоил знания, необходимые для организации защиты информации Обучающийся подготовил и представил доклад, в котором на основе анализа различных источников информации, информационных ресурсов самостоятельно освоил знания, необходимые для организации защиты информации

Опрос: описание показателей и критериев оценивания компетенций
Оценка Не зачтено Зачтено
Оценивается знание и умение раскрыть содержание основных категорий и понятий по организационной защите инофрмации.
Набранная сумма баллов (% выполненных заданий –правильно сформулированных терминов) (мах – 100) Менее 60 60 -100

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.1	Спицын В. Г.	Информационная безопасность вычислительной техники: учебное пособие (https://biblioclub.ru/index.php?page=book&id=208694)	Томск : Эль Контент, 2011	ЭБС
Л1.2	Рытенкова О.	Информационная безопасность: журнал (https://biblioclub.ru/index.php?page=book&id=211297)	Москва : ГРОТЕК, 2012	ЭБС
Л1.3	Рытенкова О.	Информационная безопасность: журнал (https://biblioclub.ru/index.php?page=book&id=211298)	Москва : ГРОТЕК, 2012	ЭБС
Л1.4	Рытенкова О.	Информационная безопасность: журнал (https://biblioclub.ru/index.php?page=book&id=211299)	Москва : ГРОТЕК, 2012	ЭБС
Л1.5	Прохорова О. В.	Информационная безопасность и защита информации: учебник (https://biblioclub.ru/index.php?page=book&id=438331)	Самара : Самарский государственный архитектурно-строительный университет, 2014	ЭБС

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.6	Зенков А. В.	Информационная безопасность и защита информации: учебное пособие для вузов (https://urait.ru/bcode/477968)	Москва : Юрайт, 2021	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Каторин Ю. Ф., Разумовский А. В., Спивак А. И.	Защита информации техническими средствами: учебное пособие (http://e.lanbook.com/books/element.php?pl1_id=40850)	Санкт- Петербург : НИУ ИТМО, 2012	ЭБС
Л2.2	Сергеева Ю. С.	Защита информации: конспект лекций: учебное пособие (https://biblioclub.ru/index.php?page=book&id=72670)	Москва : А-Приор, 2011	ЭБС
Л2.3	Трищенко С.	Секретная информация: сборник фантастических рассказов: художественная литература (https://biblioclub.ru/index.php?page=book&id=259017)	Екатеринбург : Аэлита, 2013	ЭБС
Л2.4	Ковалев Д.В., Богданова Е.А.	Информационная безопасность: учебное пособие (http://znanium.com/catalog/document?id=330789)	Ростов-на-Дону : Издательство Южного федерального университета (ЮФУ), 2016	ЭБС
Л2.5	Клименко И.С.	Информационная безопасность и защита информации: модели и методы управления: монография (http://znanium.com/catalog/document?id=360289)	Москва : ООО "Научно-издательский центр ИНФРА-М", 2021	ЭБС
Л2.6	Глинская Е.В., Чичварин Н.В.	Информационная безопасность конструкций ЭВМ и систем: учебное пособие (http://znanium.com/catalog/document?id=362430)	Москва : ООО "Научно-издательский центр ИНФРА-М", 2021	ЭБС
Л2.7	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: учебное пособие (http://znanium.com/catalog/document?id=364622)	Москва : Издательский Дом "ФОРУМ", 2021	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Лань [Электронный ресурс]: электронно-библиотечная система (ЭБС) / издательство Лань. - URL: http://e.lanbook.com/
Э2	Университетская библиотека онлайн [Электронный ресурс]: электронно-библиотечная система (ЭБС) / ООО Директмедиа Паблишинг. - URL: http://biblioclub.ru/
Э3	Юрайт [Электронный ресурс]: электронно-библиотечная система (ЭБС) / издательство Юрайт. - URL: https://urait.ru/
Э4	Znanium.com [Электронный ресурс]: электронно-библиотечная система (ЭБС) / Научно-издательский центр ИНФРА-М. - URL: http://znanium.com/
Э5	eLIBRARY.RU [Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. – URL: http://elibrary.ru/defaultx.asp

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

MS Office365

Adobe Reader

LMS Moodle

Android Studio

Adobe Connect Acrobat

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. Научная электронная библиотека eLIBRARY.RU (https://elibrary.ru/defaultx.asp?) eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: https://elibrary.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. Справочно-правовая система «КонсультантПлюс» (http://www.consultant.ru/) КонсультантПлюс : справочно- правовая система : база данных / Региональный центр правовой информации Информправо. – Москва, 1992 – . – Режим доступа: из читальных залов библиотеки. – Текст : электронный.

3. Справочно-правовая система «Гарант» (http://www.garant.ru/) ГАРАНТ.РУ : информационно-правовой портал / ООО «НПО ГАРАНТ-СЕРВИС». – Москва, 1990 – . – Режим доступа: из читальных залов библиотеки 1-го корпуса (читальный зал № 3 – ауд. 205, медиацентр – ауд. 206, библиотека юридической литературы – ауд. 215). – Текст : электронный.

4. Национальная электронная библиотека (НЭБ) (https://rusneb.ru/) Национальная электронная библиотека (НЭБ) : объединенный электронный каталог фондов российских библиотек : сайт. – URL: http://нэб.рф. – Режим доступа: из читальных залов библиотеки ЧелГУ. – Текст : электронный.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для реализации дисциплины используются учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения: доска, парты, мультимедийное и аудио оборудование.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно- наглядных пособий: цифровые образовательные ресурсы, мультимедийный проектор, переносное и /или стационарное мультимедийное оборудование (ноутбук, проектор, колонки).

Для проведения семинарских занятий используются аудитории, оснащенные обычной доской, партами, переносным мультимедийным оборудованием (ноутбук, проектор, колонки).

Для самостоятельной работы студента используются аудитория №205 - читальный зал №3 (учебный корпус №1) и аудитория №206 - электронный читальный зал (специализированный медиацентр) (учебный корпус №1), оснащенные персональными компьютерами, мультимедийной аппаратурой. В аудиториях обеспечен доступ к различной справочной литературе, энциклопедиям, библиографическим и полнотекстовым базам данных, информационным ресурсам «Интернет».

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Изучение учебной дисциплины «Организационное и правовое обеспечение информационной безопасности» требует от студента серьёзного и добросовестного отношения к овладению специальными знаниями, необходимыми для становления качественно нового уровня юридического образования и практики.

Сложности, которые возникают в ходе аудиторной и внеаудиторной работы, объясняются большим объёмом подлежащего освоению учебного материала и необходимостью тщательной самостоятельной подготовки. Эффективному освоению материала учебной дисциплины способствует внимательная проработка лекционного материала, позволяющая сформировать целостное представление относительно основных закономерностей административной деятельности органов внутренних дел.

Лекционный курс охватывает наиболее значимые вопросы каждой темы изучения. Уяснение лекционного материала контролируется устным опросом и тестированием. Изучение проблем каждого раздела дисциплины продолжается в ходе подготовки и участия в практических занятиях.

Форма проведения практического занятия объявляется студентам заранее.

Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, социальных сетей и т.п.

Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.

Виды самостоятельной работы:

– конспектирование подзаконных нормативно-правовых источников;

– проработка учебного материала (по конспектам лекций, учебной и научной литературе) и подготовка докладов для практических занятий;

– работа с юридическими источниками и законодательной базой;

– написание творческих работ (эссе);

– работа с тестами и вопросами для самопроверки.

Результаты самостоятельной работы контролируются преподавателем и учитываются при текущей аттестации студента. При этом проводятся: тестирование, экспресс-опрос на практических занятиях, заслушивание докладов, проверка письменных работ и т.д.

Несомненно, умение анализировать юридические источники, работать с литературой, навыки поиска, обработки и оформления необходимой информации, способность обосновывать собственную позицию помогут студенту в дальнейшей самостоятельной учебной и научной работе.

В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных

технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции (вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, MS Office365, форумы, электронная почта и др.).
При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.
Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и голо информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося.
1. Мобильные специальные технические средства для лиц с нарушениями зрения: портативный компьютер с вводом/выводом шрифтом Брайля с синтезатором речи «ElBraile-W14J G2»; ноутбуки с программной экранного доступа NVDA; электронные увеличители для удаленного просмотра; видеоувеличители портативные; тифлоплеер; цифровые диктофоны.
2. Мобильные специальные технические средства для лиц с нарушениями слуха: система свободного звукового поля со встроенной совместимостью с FM-устройствами; радиоклассы «Сонет-РСМ» с передатчиком, заушным индуктором и индукционной петлей; система информационная для слабослышащих переносная «Исток» А2 со встроенным плеером – звуковым информатором; документ-камера; программируемые слуховые аппараты индивидуального пользования.
3. Ассистивные информационные технологии: программное обеспечение экранного доступа с синтезом речи NVDA; программы экранного увеличения; программы речевого синтеза для компьютеров и ноутбуков; программы речевого синтеза для мобильных устройств; экранная клавиатура; экранная лупа.
При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации NVDA, речевые синтезаторы, экранные лупы).
В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом нарушений их здоровья.
Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах, с помощью специальных технических и программных средств (рабочее место для незрячего пользователя с программным обеспечением экранного доступа с синтезом речи NVDA, рабочее место с компьютерным роллером и клавиатурой Clevy с большими кнопками и с разделяющей клавиши накладкой).
Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:
Для лиц с нарушениями зрения:
- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме шрифтом Брайля.
Для лиц с нарушениями слуха:
- в печатной форме,
- в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата:
- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий (Moodle, Adobe Connect Pro и пр.).

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья используется индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации направлены на индивидуализацию обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей, обучающихся:

а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, в письменной форме шрифтом Брайля, устно с использованием услуг сурдопереводчика);

б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);

в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.