Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Национальный исследовательский университет «МЭИ»
в г. Смоленске

УТВЕРЖДАЮ
Зам. директора
по учебно-методической работе
филиала ФГБОУ ВО
«НИУ «МЭИ» в г. Смоленске
_____ В.В. Рожков
«11» 10 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: 10.04.01 Информационная безопасность

Магистерская программа: Безопасность автоматизированных систем

Уровень высшего образования: магистратура

Нормативный срок обучения: 2 года

Форма обучения: очная

Год набора: 2022

Смоленск

Программа составлена с учетом ФГОС ВО – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от «26» ноября 2020 г. № 1455

Программу составил:

д-р экон. наук, проф. _____ _____Л.В. Фомченкова_____
подпись ФИО

«28» _____09_ 2021 г.

Программа обсуждена и одобрена на заседании кафедры информационных технологий в экономике и управлении
«29» ____09_ 2021 г., протокол № 1

Заведующий кафедрой информационных технологий в экономике и управлении:

_____ __д-р техн. наук, проф._М.И. Дли_____
подпись ФИО

«08» _____октября____ 2021 г.

Согласовано:

Заведующий кафедрой вычислительной техники:

____ _____ __д-р техн. наук, проф._А.С. Федулов_____
подпись ФИО

«08» _____октября____ 2021 г.

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Ответственный в филиале по работе
с ЛОВЗ и инвалидами

_____ _____Е.В. Зуева_____
подпись ФИО

«08» _____октября____ 2021 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является подготовка обучающихся к решению задач профессиональной деятельности организационно-управленческого типа в области защиты информации по направлению подготовки 10.04.01 Информационная безопасность (магистерская программа: Безопасность автоматизированных систем) посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС и установленных программой магистратуры на основе профессиональных стандартов, в части представленных ниже знаний, умений и навыков.

Задачи дисциплины:

- ознакомить обучающихся со структурой, видами и спецификой информационно-правовых норм, международными и отечественными стандартами в области безопасности информационных систем и технологий; основами законодательства Российской Федерации в области информационной безопасности; конституционными гарантиями защиты информационных прав; особенностями организационных мер обеспечения безопасности информационных систем;
- сформировать умения извлекать, систематизировать и критически переосмысливать информацию по нормативно-правовым документам, международным и отечественным стандартам в области информационных систем и технологий из различных источников; обосновывать состав, характеристики и функциональные возможности систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; формулировать требования к проектным решениям по видам обеспечения информационных систем по соблюдению норм законодательства РФ в области информационной безопасности; разрабатывать организационные меры по обеспечению политики информационной безопасности;
- выработать практические навыки поиска и анализ информации в современных информационных справочно-правовых системах; организации выполнения работ с учетом требований информационной безопасности; поиска, анализа и применения нормативных актов, необходимых для обоснования требований к проектным решениям и разработке организационных мер обеспечения политики информационной безопасности; выбора систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина Организационно-правовые механизмы обеспечения информационной безопасности относится *к части, формируемой участниками образовательных отношений.*

Перечень последующих дисциплин, для которых необходимы знания, умения и навыки, формируемые данной дисциплиной:

Б1.В.04 Информационная безопасность компьютерных сетей
Б1.В.07 Технические средства защиты информации
Б1.В.ДВ.02.01 Комплексная защита корпоративной информации
Б1.В.ДВ.02.02 Аудит информационной безопасности
Б1.В.ДВ.03.01 Безопасность веб-приложений
Б1.В.ДВ.03.02 Технологии и методы защиты информации в сети Интернет
Б2.В.02 (П) Проектно-технологическая практика
Б2.В.03 (П) Преддипломная практика
Б3.01 Подготовка к защите и защита выпускной квалификационной работы

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины направлено на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОП ВО по данному направлению подготовки:

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы достижения компетенций	Результаты обучения
ПК-3 Способен управлять безопасностью компьютерных систем и сетей	ПК-3.1 Проводит анализ безопасности компьютерных систем и сетей	Знает: структуру, виды и специфику информационно-правовых норм, международные и отечественные стандарты в области безопасности информационных систем и технологий Умеет: извлекать, систематизировать и критически переосмысливать информацию по нормативно-правовым документам, международным и отечественным стандартам в области информационных систем и технологий из различных источников, обосновывать состав, характеристики и функциональные возможности систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов Владеет: навыками поиска и анализ информации в современных информационных справочно-правовых системах, организации выполнения работ с учетом требований информационной безопасности
	ПК-3.2 Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей	Знает: основы законодательства Российской Федерации в области информационной безопасности; конституционные гарантии защиты информационных прав, особенности организационных мер обеспечения безопасности информационных систем Умеет: формулировать требования к проектным решениям по видам обеспечения информационных систем по соблюдению норм законодательства РФ в области информационной безопасности, разрабатывать организационные меры по обеспечению политики информационной безопасности Владеет: навыками поиска, анализа и применения нормативных актов, необходимых для обоснования требований к проектным решениям и разработке организационных мер обеспечения политики информационной безопасности, навыками выбора систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Структура дисциплины:

№	Индекс	Наименование	Семестр 1										Семестр 2										Итого за курс										Каф.	Семестры
			Контроль	Академических часов								з.е.	Недель	Контроль	Академических часов								з.е.	Недель	Контроль	Академических часов								з.е.	Недель		
				Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Конт роль				Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Конт роль				Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Конт роль	Всего			
8	Б1.В.01	Организационно-правовые механизмы обеспечения информационной безопасности	ЗаО Реф	**108**	68	34	34			31	9	3													ЗаО Реф	**108**	68	34	34			31	9	3		20	1

ОБОЗНАЧЕНИЯ:
Виды промежуточной аттестации (виды контроля):
Экз - экзамен;
ЗаО - зачет с оценкой;
За – зачет;
Виды работ:
Контакт. – контактная работа обучающихся с преподавателем;
Лек. – лекционные занятия;
Лаб.– лабораторные работы;
Пр. – практические занятия;
КРП – курсовая работа (курсовой проект);
РГР – расчетно-графическая работа (реферат);
СР – самостоятельная работа студентов;
з.е.– объем дисциплины в зачетных единицах.

Содержание дисциплины:

№	Наименование видов занятий и тематик, содержание
1	Лекционные занятия 17 шт. по 2 часа: 1.1. Организационно-правовое обеспечение информационной безопасности в условиях цифровой трансформации 1.2. Организационные механизмы государственного управления в сфере информационной безопасности. 1.3. Электронное правительство и обеспечение информационной безопасности 1.4. Механизмы организационно-правового обеспечения безопасности информационной инфраструктуры РФ 1.5. Организационно-правовые механизмы защиты информационных систем 1.6. Организационно-правовые механизмы защиты информации 1.7. Механизм охраны авторских и смежных прав в сфере информатики 1.8. Организационно-правовой механизм защиты государственной тайны в РФ 1.9. Организационно-правовой механизм защиты служебной тайны в РФ 1.10. Организационно-правовой механизм защиты коммерческой тайны в РФ 1.11. Организационно-правовой механизм защиты банковской тайны в РФ 1.12. Правовое и нормативное регулирование деятельности в области обеспечения безопасности персональных данных 1.13. Организационно-функциональные документы системы информационной безопасности 1.14. Организация службы защиты информации 1.15. Задачи и функции управления службой информационной безопасности организации 1.16. Информационная и ментальная войны: сущность и механизмы противоборства 1.17. Организационно-правовые механизмы международной информационной безопасности
2	Лабораторные работы 8 шт. по 4 часа и 1 шт. – 2 часа: 2.1. Законодательство РФ в сфере информационной безопасности (4 часа) 2.2. Государственная система обеспечения информационной безопасности (4 часа) 2.3. Правовая охрана компьютерных программ и баз данных (4 часа) 2.4. Законодательство РФ в области защиты государственной и служебной тайны (4 часа) 2.5. Юридическая защита и ответственность за нарушение прав на коммерческую и банковскую тайну (4 часа) 2.6. Правовая защита персональных данных (4 часа) 2.7. Лицензирование деятельности службы информационной безопасности организации (4 часа) 2.8. Разработка документов службы информационной безопасности организации (4 часа) 2.9. Построение структурной схемы управления службой информационной безопасности организации (2 часа)
3	Реферат Темы реферата: 3.1. Сертификация средств защиты информации и аттестации объектов информатизации 3.2. Информационное оружие и механизмы противодействия 3.3. Сущность, методы и формы организационной защиты информации 3.4. Организация защиты конфиденциальной информации. 3.5. Организация защиты государственной тайны в РФ. 3.6. Организация защиты информации при осуществлении международного

№	Наименование видов занятий и тематик, содержание
	сотрудничества. 3.7. Аналитическая работа как основа управления системой организационной защиты информации. 3.8. Функциональная направленность режима информационной безопасности объекта 3.9. Понятие информационной безопасности в российском и зарубежном законодательстве 3.10. Организация защиты интеллектуальной собственности и авторское право в российском законодательстве 3.11. Обеспечение защиты персональных данных при формировании Единого федерального информационного регистра 3.12. Информационная война: цели, задачи, объект, субъект. 3.13. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание 3.14. Организационно-правовое обеспечение информационной безопасности экономического субъекта 3.15. Организационно-правовые основы сертификации и аттестации средств защиты информации
4	Самостоятельная работа студентов: 4.1. Разработка и реализация механизма организационно-правового обеспечения политики информационной безопасности корпоративных информационных систем: понятие политики информационной безопасности государственных и коммерческих структур; основные функции службы информационной безопасности; организационно-методологические основы реализации политики информационной безопасности с применением стандартов систем менеджмента информационной безопасности. 4.2. Информационное противоборство и обеспечение информационной безопасности на межгосударственном уровне: информационное противоборство как способ разрешения межгосударственных противоречий; информационная война: цели, задачи, объект, субъект; дезинформация: сущность, способы обнаружения и противодействия; механизмы обеспечения международной информационной безопасности. 4.3. Самостоятельная работа по теме реферата

Текущий контроль:

Индикаторы достижения компетенции	Вид текущего контроля	Тема
ПК-3.1 Проводит анализ безопасности компьютерных систем и сетей	Защита лабораторных работ Проверка конспектов лекций и дополнительных материалов Проверка реферата	1.1. Организационно-правовое обеспечение информационной безопасности в условиях цифровой трансформации 1.3. Электронное правительство и обеспечение информационной безопасности 1.4. Механизмы организационно-правового обеспечения безопасности информационной инфраструктуры РФ 1.5. Организационно-правовые механизмы защиты информационных систем 1.6. Организационно-правовые механизмы защиты информации 1.7. Механизм охраны авторских и смежных прав в сфере информатики

Индикаторы достижения компетенции	**Вид текущего контроля**	**Тема**
		1.8. Организационно-правовой механизм защиты государственной тайны в РФ 1.9. Организационно-правовой механизм защиты служебной тайны в РФ 1.10. Организационно-правовой механизм защиты коммерческой тайны в РФ 1.11. Организационно-правовой механизм защиты банковской тайны в РФ 1.12. Правовое и нормативное регулирование деятельности в области обеспечения безопасности персональных данных 1.13. Организационно-функциональные документы системы информационной безопасности 1.16. Информационная и ментальная войны: сущность и механизмы противоборства 2.1. Законодательство РФ в сфере информационной безопасности 2.2. Государственная система обеспечения информационной безопасности 2.3. Правовая охрана компьютерных программ и баз данных 2.4. Законодательство РФ в области защиты государственной и служебной тайны 2.5. Юридическая защита и ответственность за нарушение прав на коммерческую и банковскую тайну 2.6. Правовая защита персональных данных 4.2. Информационное противоборство и обеспечение информационной безопасности на межгосударственном уровне
ПК-3.2 Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей	ПК-3.2 Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей	1.2. Организационные механизмы государственного управления в сфере информационной безопасности. 1.14. Организация службы защиты информации 1.15. Задачи и функции управления службой информационной безопасности организации 1.17. Организационно-правовые механизмы международной информационной безопасности 2.7. Лицензирование деятельности службы информационной безопасности организации 2.8. Разработка документов службы информационной безопасности организации 2.9. Построение структурной схемы управления службой информационной безопасности организации 4.1. Разработка и реализация механизма организационно-правового обеспечения политики информационной безопасности корпоративных информационных систем

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Таблица - Образовательные технологии, используемые при реализации различных видов учебной занятий по дисциплине

№ п/п	Виды учебных занятий	Образовательные технологии
1	Лекции	Интерактивная лекция (лекция-визуализация) Индивидуальные и групповые консультации по дисциплине
2	Лабораторная работа	Технология выполнения лабораторных заданий индивидуально
3	Самостоятельная работа студентов (внеаудиторная)	Информационно-коммуникационные технологии (доступ к ЭИОС филиала, к ЭБС филиала, доступ к информационно-методическим материалам по дисциплине)
4	Контроль (промежуточная аттестация: зачет)	Технология устного опроса

6. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ – ДЛЯ ОЦЕНКИ КАЧЕСТВА ОСВОЕНИЯ ДИСЦИПЛИНЫ

К промежуточной аттестации студентов по дисциплине могут привлекаться представители работодателей, преподаватели последующих дисциплин, заведующие кафедрами.

Оценка качества освоения дисциплины включает как текущий контроль успеваемости, так и промежуточную аттестацию.

Лабораторная работа «Законодательство РФ в сфере информационной безопасности»

1. Какие законы и законодательные акты РФ регламентируют вопросы упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей?
2. Какие меры наказания за нарушение законодательства Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей предусмотрены Кодексом Российской Федерации об административных правонарушениях?
3. Дайте определение понятия электронный документ, электронная цифровая подпись.
4. Сфера применения и основные положения федерального закона "Об электронной подписи" N 63-ФЗ. При выполнении каких условий в соответствии с российским законодательством электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе? Какие условия должны быть выполнены для признания

Лабораторная работа «Государственная система обеспечения информационной безопасности»

1. На каких принципах основывается государственная политика обеспечения информационной безопасности России?
2. Для чего предназначена система обеспечения информационной безопасности России?

3. Перечислите основные функции системы обеспечения информационной безопасности России
4. Что включает в себя система правового обеспечения информационной безопасности России?

Лабораторная работа «Правовая охрана компьютерных программ и баз данных»

1. Какие правовые акты общего назначения, затрагивающие вопросы информационной безопасности, вы знаете?
2. Дать определения следующих понятий: автор, правообладатель, личные неимущественные права, авторство и исключительные права на результат интеллектуальной деятельности, служебное произведение.
3. Назовите принципы засекречивания информации.
4. Какие основания предусмотрены для рассекречивания информации?

Лабораторная работа «Законодательство РФ в области защиты государственной и служебной тайны»

1. Сфера применения и основные положения федерального закона «О государственной тайне» (закон РФ N 5485-1).
2. Сфера применения и основные положения федерального закона «О безопасности» (закон РФ N 390-ФЗ).
3. Какая административная ответственность предусмотрена за нарушение законодательства РФ в области защиты государственной тайны?
4. Какая уголовная ответственность предусмотрена за нарушение законодательства РФ в области защиты государственной тайны?

Лабораторная работа «Юридическая защита и ответственность за нарушение прав на коммерческую и банковскую тайну»

1. Сфера применения и основные положения федерального закона «О коммерческой тайне» № 98-ФЗ.
2. По каким признакам информация может быть отнесена к коммерческой тайне? Какие сведения не являются коммерческой тайной?
3. Какая информация может быть отнесена к банковской тайне?
4. Какая административная и уголовная ответственность предусмотрена за нарушение законодательства РФ в области защиты банковской тайны?

Лабораторная работа «Правовая защита персональных данных».

1. Какие основные нормативные правовые акты регулируют правовые отношения в области защиты персональных данных?
2. Каковы права субъектов персональных данных?
3. Назовите обязанности оператора персональных данных.
4. Какие административные меры предусмотрены за нарушения российского законодательства по обработке персональных данных?
5. Какова уголовная ответственность за нарушения российского законодательства по обработке персональных данных?

Лабораторная работа «Лицензирование деятельности службы информационной безопасности организации».

1. В чем состоит суть лицензирования деятельности организации в области защиты информации?

2. Какие виды деятельности организации в области защиты информации необходимо лицензировать?
3. Перечислите основные нормативные документы, регламентирующие деятельность в области защиты информации

Лабораторная работа «Разработка уставных документов службы информационной безопасности организации»

1. Какими инструкциями руководствуются при организации работы службы информационной безопасности?
2. Что необходимо включать в коллективный договор для правого обеспечения защиты информации?
3. Назовите разделы устава службы информационной безопасности организации.

Лабораторная работа «Построение структурной схемы управления службой информационной безопасности организации»

1. Какие подразделения входят в состав службы информационной безопасности организации?
2. Каким законом регламентируются функции службы информационной безопасности организации?
3. Какие задачи решает совет по информационной безопасности организации?

Результаты текущего контроля по вышеуказанным в разделе 4 видам фиксируются с использованием трехбалльной системы (0, 1, 2) в виде контрольных недель - при принятой в филиале системе на 6-й и 12-й учебной неделе семестра, а также учитываются преподавателем при осуществлении промежуточной аттестации по настоящей дисциплине.

Форма промежуточной аттестации по настоящей дисциплине – *зачет с оценкой в 1-м семестре.*

Вопросы по закреплению теоретических знаний, умений и практических навыков, предусмотренных компетенциями (вопросы к зачету)

1. Предмет и методы информационного права.
2. Международный характер информационного права. Правовое регулирование информационных отношений за рубежом.
3. Система и принципы информационного права. Виды источников информационного права.
4. Государственное управление в информационной сфере.
5. Система и полномочия органов государственной власти, обеспечивающих право доступа к информации.
6. Электронное государство.
7. Государственное регулирование отношений в сфере интеллектуальной собственности.
8. Авторское право. Субъект (автор) и объекты авторского права. Охраняемые результаты интеллектуальной деятельности.
9. Личные неимущественные права, авторство и исключительные права на результат интеллектуальной деятельности. Сроки действия исключительных и личных неимущественных прав. Понятие служебного произведения.

10. Смежные права. Субъекты и объекты смежных прав. Личные неимущественные и исключительные смежные права, сроки их действия.
11. Программы для ЭВМ и базы данных как охраняемые результаты интеллектуальной деятельности.
12. Компьютерное пиратство: разновидности и методы борьбы с ним.
13. Понятие государственной тайны. Принципы засекречивания информации.
14. Понятие государственной тайны. Основания рассекречивания информации.
15. Уголовно-правовая защита информации, составляющей государственную тайну.
16. Система и компетенция органов, обеспечивающих охрану государственной тайны.
17. Служебная тайна. Признаки отнесения сведений к служебной тайне.
18. Правовой режим отдельных видов информации, составляющей служебную тайну.
19. Профессиональная тайна. Критерии охраноспособности. Правовой режим отдельных видов информации, составляющей профессиональную тайну.
20. Правовые основы защиты коммерческой тайны.
21. Понятие коммерческой тайны. Признаки информации как коммерческой тайны. Сведения, не являющиеся коммерческой тайной.
22. Понятие банковской тайны. Законодательная база. Объекты и субъекты права на банковскую тайну.
23. Информация, относимая к банковской тайне. Ответственность за разглашение банковской тайны.
24. Законодательство РФ в области защиты персональных данных.
25. Основные понятия: персональные данные, оператор персональных данных, обработка персональных данных, информационная система персональных данных (ИСПД), регуляторы.
26. Категории персональных данных.
27. Права субъектов персональных данных.
28. Обязанности оператора персональных данных.
29. Административная и уголовная ответственность за нарушения российского законодательства по обработке персональных данных.
30. Автоматизированная и неавтоматизированная обработка персональных данных. Особенности обеспечения безопасности персональных данных в автоматизированных ИСПД.
31. Обеспечение безопасности персональных данных при их обработке в ИСПД.
32. Понятие электронного документа. Нормативно-правовое регулирование электронного документооборота.
33. Электронная цифровая подпись.
34. Общие положения организационной защиты.
35. Служба безопасности организации.

Пример практических заданий, выносимых на зачет, для проверки практических умений и навыков студентов по дисциплине

Вы работаете IT-специалистом в компании, которая организовала в своем офисе в зале по работе с клиентами публичный WiFi с доступом в Интернет. В настоящий момент доступ в Интернет через WiFi организован без использования паролей простым выбором сети и принятием условий пользования Интернет.

Обеспечивает ли существующий алгоритм доступа в Интернет для клиентов компании требования законодательства Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей?

Какие способы идентификации клиента разрешены без предоставления удостоверяющих документов?

В филиале используется система с традиционной шкалой оценок – "отлично", "хорошо", "удовлетворительно", "неудовлетворительно", "зачтено", "не зачтено".

Применяемые критерии оценивания по дисциплинам (в соответствии с инструктивным письмом НИУ МЭИ от 14 мая 2012 года № И-23):

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, обнаружившему всестороннее, систематическое и глубокое знание материалов изученной дисциплины, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной рабочей программой дисциплины; проявившему творческие способности в понимании, изложении и использовании материалов изученной дисциплины, безупречно ответившему не только на вопросы билета, но и на дополнительные вопросы в рамках рабочей программы дисциплины, правильно выполнившему практическое задание. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущего контроля. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «эталонный».
«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, обнаружившему полное знание материала изученной дисциплины, успешно выполняющему предусмотренные задания, усвоившему основную литературу, рекомендованную рабочей программой дисциплины; показавшему систематический характер знаний по дисциплине, ответившему на все вопросы билета, правильно выполнивший практическое задание, но допустивший при этом непринципиальные ошибки. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущего контроля. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «продвинутый».
«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	Выставляется обучающемуся, обнаружившему знание материала изученной дисциплины в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением заданий, знакомому с основной литературой, рекомендованной рабочей программой дисциплины; допустившему погрешность в ответе на теоретические вопросы и/или при выполнении практических заданий, но обладающему необходимыми знаниями для их устранения под руководством преподавателя, либо неправильно выполнившему практическое задание, но по указанию преподавателя выполнившему другие практические задания из того же раздела дисциплины.. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «пороговый».
«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, обнаружившему серьезные пробелы в знаниях основного материала изученной дисциплины, допустившему принципиальные ошибки в выполнении заданий, не ответившему на все вопросы билета и дополнительные вопросы и неправильно выполнившему практическое задание (неправильное выполнение только практического задания не является однозначной причиной для выставления оценки «неудовлетворительно»). Как правило, оценка «неудовлетворительно ставится студентам, которые не могут

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
	продолжить обучение по образовательной программе без дополнительных занятий по соответствующей дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущего контроля. Компетенции на уровне «пороговый», закреплённые за дисциплиной, не сформированы.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебное и учебно-лабораторное оборудование

Для проведения лекционных занятий

Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная:

- специализированной мебелью; доской аудиторной; демонстрационным оборудованием: персональным компьютером (ноутбуком); переносным (стационарным) проектором.

Для проведения занятий лабораторного типа

Учебная аудитория для лабораторных работ, выполняемых в компьютерном классе, оснащенная:

- специализированной мебелью; доской аудиторной; персональными компьютерами с подключением к сети "Интернет" и доступом в ЭИОС филиала.

Для самостоятельной работы обучающихся по дисциплине используется помещение для самостоятельной работы обучающихся, оснащенное:

- специализированной мебелью; доской аудиторной; персональным компьютерами с подключением к сети "Интернет" и доступом в ЭИОС филиала.

Программное обеспечение

При проведении лекционных занятий предусматривается использование программного обеспечения Microsoft Office (система для подготовки и проведения презентаций Microsoft Power Point).

При проведении **лабораторных работ** предусматривается использование программного обеспечения Microsoft Office (текстовый редактор Microsoft Word).

При написании **реферата** предусматривается использование обучающимися программного обеспечения Microsoft Office (текстовый редактор Microsoft Word).

8. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

для глухих и слабослышащих:

- лекции оформляются в виде электронного документа;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере;
- используется специальная учебная аудитория для лиц с ЛОВЗ – ауд. 106 главного учебного корпуса по адресу 214013, г. Смоленск, Энергетический пр-д, д.1, здание энергетического института (основной корпус).

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены филиалом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается **доступ к информационным и библиографическим ресурсам в сети Интернет** для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;

- в форме электронного документа;
- в форме аудиофайла.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература.

1 Новиков В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс] : учебное пособие. — Москва : Горячая линия-Телеком, 2017. — 176 с. — Режим доступа: https://e.lanbook.com/book/111084.

Дополнительная литература.

1 Ковалев Д.В. Информационная безопасность [Электронный ресурс] : учебное пособие / Д.В. Ковалев, Е.А. Богданова. — Ростов-на-Дону : Издательство Южного федерального университета, 2016. — 74 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=493175.

2 Бекетнова Ю.М. Международные основы и стандарты информационной безопасности финансово-экономических систем [Электронный ресурс] : учебное пособие / Ю.М. Бекетнова, Г.О. Крылов, С.Л. Ларионова ; Финансовый университет при Правительстве Российской Федерации. — Москва : Прометей, 2018. — 173 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=494850.

3 Аверченков В.И. Служба защиты информации: организация и управление [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. — 3-е изд., стер. — Москва : Издательство «Флинта», 2016. — 186 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=93356.

Список авторских методических разработок.

Фомченкова Л.В. Методические указания к занятиям по дисциплине «Организационно-правовые механизмы обеспечения информационной безопасности» [Электронный ресурс]: электронные методические указания для студентов, обучающихся по направлению 10.04.01 «Информационная безопасность» / Фомченкова Л.В. – Электрон. дан. – Смоленск: РИО филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2019.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет» необходимых для освоения дисциплины

1 Справочная правовая система Консультант плюс [электронный ресурс] — Режим доступа : http://www.consultant.ru/online/.

2 Официальный сайт Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) [электронный ресурс] — Режим доступа : http://government.ru/department/387/events/.

3 Официальный сайт Федеральной службы по интеллектуальной собственности — Режим доступа : https://rospatent.gov.ru/ru

4 Официальный сайт ФСТЭК РФ [электронный ресурс] — Режим доступа : https://fstec.ru/

5 Официальный сайт Верховного суда РФ [электронный ресурс] — Режим доступа : http://www.supcourt.ru/

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Номера страниц				Всего страниц в документе	Наименование и № документа, вводящего изменения	Подпись, Ф.И.О. внесшего изменения в данный экземпляр	Дата внесения изменения в данный экземпляр	Дата введения изменения
	измененных	замененных	новых	аннулированных					
1	2	3	4	5	6	7	8	9	10