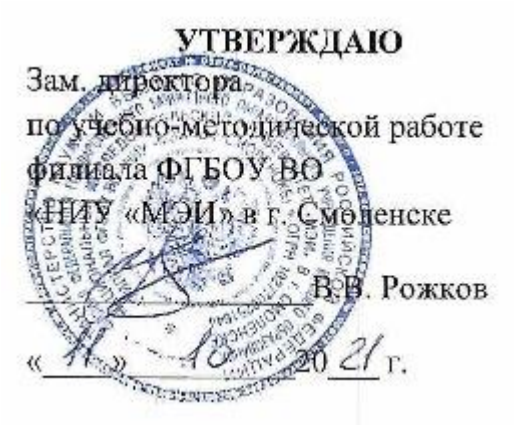
Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Национальный исследовательский университет «МЭИ»
в г. Смоленске



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

(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:

канд. экон. наук, доц. _____ О.В. Булыгина
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» 10 2021 г.

Согласовано:

Заведующий кафедрой вычислительной техники:

_____ _____ д-р техн. наук, проф. А.С. Федулов
подпись ФИО

«08» 10 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» 10 2021 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является подготовка обучающихся к решению задач профессиональной деятельности организационно-управленческого, проектного и научно-исследовательского типов 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 с российскими нормативными правовыми документами, международными и отечественными стандартами в области обеспечения информационной безопасности;
- дать представление об угрозах, рисках и уязвимостях информационной безопасности;
- сформировать умение проводить анализ проблем информационной безопасности;
- сформировать навыки разработки концепции и политики информационной безопасности;
- сформировать умение разрабатывать стратегию построения и внедрения системы управления информационной безопасностью;
- сформировать практические навыки разработки технического задания на создание системы обеспечения информационной безопасности;
- научить выполнять оценку экономической эффективности системы обеспечения информационной безопасности предприятия.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина Управление информационной безопасностью относится *к обязательной части программы*.

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

Б1.О.04 Планирование научного эксперимента
Б1.О.05 Технологии обеспечения информационной безопасности
Б1.О.07 Защищенные информационные системы
Б2.В.01(Н) Научно-исследовательская работа
ФТД.02 Информационная безопасность цифровой экономики

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
УК-1. Способен осуществлять критический анализ	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее	Знает: методы обследования организации. Умеет: проводить анализ проблем информационной безопасности.

проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	составляющие и связи между ними	Владеет: навыками анализа и формирования причинно-следственных связей в исследуемой проблеме.
	УК-1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению	Знает: критерии качества информации. Умеет: формировать критерии для поиска информации для решения исследуемой проблемы. Владеет: навыками устранения пробелов в информации, необходимой для решения исследуемой проблемы.
	УК-1.3 Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников	Знает: виды информационных ресурсов. Умеет: критически оценивать надежность источников информации. Владеет: навыками работы с различными источниками информации, необходимой для решения исследуемой проблемы.
	УК-1.4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов	Знает: принципы системного и процессного подхода к управлению информационной безопасностью. Умеет: планировать систему управления информационной безопасностью. Владеет: навыками выбора подхода к внедрению системы управления информационной безопасностью.
	УК-1.5 Строит сценарии реализации стратегии, определяя возможные риски и предлагая пути их устранения	Знает: виды стратегий построения и внедрения системы управления информационной безопасностью. Умеет: разрабатывать стратегию построения и внедрения системы управления информационной безопасностью. Владеет: навыками исследования проблем реализации стратегии построения и внедрения системы управления информационной безопасностью.
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1 Обосновывает требования к системе обеспечения информационной безопасности	Знает: требования нормативных правовых актов и методических документов для рассматриваемого объекта информатизации. Умеет: разрабатывать требования к системе управления информационной безопасности. Владеет: навыками анализа активов организации, их угроз информационной безопасности и уязвимостей.
	ОПК-1.2 Разрабатывает проект технического задания на создание системы обеспечения информационной безопасности	Знает: структуру и содержание технического задания на создание системы обеспечения информационной безопасности. Умеет: разрабатывать техническое задание на создание системы обеспечения информационной безопасности. Владеет: навыками выбора инструментальных средств для реализации элементов защиты информации.
ОПК-3. Способен разрабатывать	ОПК-3.1 Анализирует и структурирует информацию	Знает: состав организационно-распорядительных документов по обеспечению

проекты организационно-распорядительных документов по обеспечению информационной безопасности	необходимую для проекта организационно-распорядительных документов по обеспечению информационной безопасности	информационной безопасности. Умеет: собирать и структурировать информацию для разработки организационно-распорядительных документов по обеспечению информационной безопасности. Владеет: навыками анализа потребностей в документальном обеспечении информационной безопасности.
	ОПК-3.2 Выбирает технологию разработки организационно-распорядительных документов	Знает: российские нормативные правовые документы, международные и отечественные стандарты в области обеспечения информационной безопасности. Умеет: выбирать стандарт, по которому будут разрабатываться организационно-распорядительные документы по обеспечению информационной безопасности. Владеет: навыками сравнительного анализа различных подходов к документальному обеспечению информационной безопасности.
	ОПК-3.3 Оформляет проект организационно-распорядительных документов по обеспечению информационной безопасности	Знает: содержание концепции и политик информационной безопасности. Умеет: определять необходимые виды частных политик информационной безопасности. Владеет: навыками разработки набора организационно-распорядительных документов по обеспечению информационной безопасности

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	Конт такт.	Лек	Лаб	Пр	КРП	СР	Конт роль				Всего	Конт такт.	Лек	Лаб	Пр	КРП	СР	Конт роль				Всего	Конт такт.	Лек	Лаб	Пр	КРП	СР	Конт роль	Всего				
3	Б1.О.03	Управление информационной безопасностью	Экз	**144**	68	34	34			40	36	4													Экз	**144**	68	34	34			40	36	4		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. Ключевые вопросы информационной безопасности. 1.2. Информационная безопасность в системе национальной безопасности России. 1.3. Стандартизация процессов управления информационной безопасностью. 1.4. Классификация угроз информационной безопасности. 1.5. Модель нарушителя информационной безопасности. 1.6. Документальное обеспечение управления информационной безопасностью. 1.7. Система управления информационной безопасностью. 1.8. Корпоративная и частные политики информационной безопасности. 1.9. Процессы управления информационной безопасностью. 1.10. Организационные вопросы управления информационной безопасностью. 1.11. Технические аспекты управления информационной безопасностью. 1.12. Программные средства управления информационной безопасностью. 1.13. Идентификация и анализ информационных рисков. 1.14. Методы управления информационными рисками. 1.15. Аудит информационной безопасности. 1.16. Оценка экономической эффективности деятельности по управлению информационной безопасностью. 1.17. Измерение информационной безопасности. Оценка зрелости процессов управления информационной безопасностью.
2	Лабораторные работы 8 шт. по 4 часа и 1 шт. – 2 часа: 2.1. Анализ бизнес-процессов предприятия (4 часа). 2.2. Анализ информационных потоков и ИТ-инфраструктуры предприятия (4 часа). 2.3. Анализ внутренних и внешних угроз информационной безопасности (4 часа). 2.4. Построение модели нарушителя (4 часа). 2.5. Анализ информационных рисков предприятия (4 часа). 2.6. Разработка концепции информационной безопасности предприятия (4 часа). 2.7. Разработка политики информационной безопасности предприятия (4 часа). 2.8. Разработка технического задания на создание системы обеспечения информационной безопасности предприятия (4 часа). 2.9. Оценка экономической эффективности системы обеспечения информационной безопасности предприятия (2 часа).
3	Самостоятельная работа студентов: 3.1. Стандарт COBIT. 3.2. Характеристики информации. 3.3. Методический документ Гостехкомиссии "Специальные требования и рекомендации по технической защите конфиденциальной информации". 3.4. Подход корпорации *Microsoft* к управлению безопасностью. 3.5. Обеспечение безопасности персональных данных.

Текущий контроль:

Индикаторы достижения компетенции	Вид текущего контроля	Тема
УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними УК-1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению УК-1.3 Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников	Защита лабораторных работ. Проверка конспектов лекций и дополнительных материалов.	1.1. Ключевые вопросы информационной безопасности. 1.2. Информационная безопасность в системе национальной безопасности России. 1.16. Оценка экономической эффективности деятельности по управлению информационной безопасностью. 1.17. Измерение информационной безопасности. Оценка зрелости процессов управления информационной безопасностью. 2.1. Анализ бизнес-процессов предприятия. 2.2. Анализ информационных потоков и ИТ-инфраструктуры предприятия. 2.9. Оценка экономической эффективности системы обеспечения информационной безопасности предприятия. 3.2. Характеристики информации.
УК-1.4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов УК-1.5 Строит сценарии реализации стратегии, определяя возможные риски и предлагая пути их устранения	Защита лабораторных работ. Проверка конспектов лекций и дополнительных материалов.	1.7. Система управления информационной безопасностью. 1.9. Процессы управления информационной безопасностью. 2.6. Разработка концепции информационной безопасности предприятия. 3.4. Подход корпорации *Microsoft* к управлению безопасностью.
ОПК-1.1 Обосновывает требования к системе обеспечения информационной безопасности ОПК-1.2 Разрабатывает проект технического задания на создание системы обеспечения информационной безопасности	Защита лабораторных работ. Проверка конспектов лекций и дополнительных материалов.	1.4. Классификация угроз информационной безопасности. 1.5. Модель нарушителя информационной безопасности. 1.10. Организационные вопросы управления информационной безопасностью. 1.11. Технические аспекты управления информационной безопасностью. 1.12. Программные средства управления информационной безопасностью. 1.13. Идентификация и анализ информационных рисков. 1.14. Методы управления информационными рисками. 2.3. Анализ внутренних и внешних угроз информационной безопасности. 2.4. Построение модели нарушителя. 2.5. Анализ информационных рисков предприятия.

		2.8. Разработка технического задания на создание системы обеспечения информационной безопасности предприятия. 3.3. Методический документ Гостехкомиссии "Специальные требования и рекомендации по технической защите конфиденциальной информации".
ОПК-3.1 Анализирует и структурирует информацию необходимую для проекта организационно-распорядительных документов по обеспечению информационной безопасности ОПК-3.2 Выбирает технологию разработки организационно-распорядительных документов ОПК-3.3 Оформляет проект организационно-распорядительных документов по обеспечению информационной безопасности	Защита лабораторных работ. Проверка конспектов лекций и дополнительных материалов.	1.3. Стандартизация процессов управления информационной безопасностью. 1.6. Документальное обеспечение управления информационной безопасностью. 1.8. Корпоративная и частные политики информационной безопасности. 1.15. Аудит информационной безопасности. 2.7. Разработка политики информационной безопасности предприятия. 3.1. Стандарт COBIT. 3.5. Обеспечение безопасности персональных данных.

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. Проектная технология.
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: экзамен)	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.

Вопросы для защиты лабораторной работы «Анализ бизнес-процессов предприятия»

1. Дайте классификацию бизнес-процессов предприятия.
2. Приведите примеры внутренних и внешних бизнес-процессов.
3. Какой тип организационной структуры реализован на исследуемом предприятии?
4. Что такое ресурсы бизнес-процесса? Какие видов они бывают?
5. Какие методы анализа бизнес-процессов существуют?

Вопросы для защиты лабораторной работы «Анализ информационных потоков и ИТ-инфраструктуры предприятия»

1. Приведите классификацию информационных потоков.
2. Какие типы информации используются на предприятии?
3. Дайте определение таким характеристикам информационного потока, как источник возникновения; направление движения; скорость передачи и приема; интенсивность.
4. Перечислите основные элементы ИТ-инфраструктуры предприятия.
5. Какие информационные системы используются на предприятии?

Вопросы для защиты лабораторной работы «Анализ внутренних и внешних угроз информационной безопасности предприятия»

1. Поясните разницу между понятиями «угроза», «уязвимость», «риск».
2. Какие виды угроз информационной безопасности наиболее характерны для рассматриваемого вида экономической деятельности?
3. Приведите классификацию источников внутренних и внешних угроз.
4. Какие существуют методы парирования угроз?
5. Приведите примеры уязвимостей.

Вопросы для защиты лабораторной работы «Построение модели нарушителя»

1. В чем разница между нарушителем и злоумышленником?
2. Каковы основные мотивы нарушения информационной безопасности?
3. Что такое рубеж защиты предприятия?
4. Приведите классификацию нарушителей согласно методике ФСТЭК.
5. Поясните выбор типа модели нарушителя.

Вопросы для защиты лабораторной работы «Анализ информационных рисков предприятия»

1. Какие международные и российские стандарты составляют нормативную базу менеджмента риска на предприятии?

2. Какова роль руководства при внедрении риск-менеджмента и в обеспечении непрерывной гарантии его эффективности?
3. Какие факторы должны быть рассмотрены при определении критериев риска?
4. Как может быть оценена величина риска?
5. Какие этапы включает в себя процесс управления рисками безопасности, предложенный корпорацией *Microsoft*?

Вопросы для защиты лабораторной работы «Разработка концепции информационной безопасности предприятия»

1. Назвать основные компоненты системы обеспечения информационной безопасности.
2. В чем заключается концептуальная разница между концепцией и политикой информационной безопасности?
3. С какой целью разрабатывается концепция информационной безопасности?
4. Какими документами определяется содержание концепции информационной безопасности?
5. Что такое объекты защиты? Приведите их классификацию.

Вопросы для защиты лабораторной работы «Разработка политики информационной безопасности предприятия»

1. В чем различие между политиками, стандартами, процедурами, руководствами информационной безопасности?
2. Опишите этапы жизненного цикла политики информационной безопасности.
3. Какие виды частных политик информационной безопасности бывают?
4. Какими российскими и международными стандартами регулируются процессы создания политики информационной безопасности?
5. В каких случаях политики информационной безопасности аннулируется?

Вопросы для защиты лабораторной работы «Разработка технического задания на создание системы обеспечения информационной безопасности предприятия»

1. Опишите основные работы по созданию системы защиты информации согласно ГОСТ Р 51583-2014.
2. Приведите классификацию информационных систем по требованиям защиты информации.
3. Перечислите функции заказчика и оператора по обеспечению защиты информации в информационной системе.
4. Охарактеризуйте типы субъектов и объектов доступа.
5. Перечислите основные меры защиты информации согласно методическому документу Гостехкомиссии "Специальные требования и рекомендации по технической защите конфиденциальной информации".

Вопросы для защиты лабораторной работы «Оценка экономической эффективности системы обеспечения информационной безопасности предприятия»

1. Какие подходы можно использовать для экономической оценки обеспечения информационной безопасности предприятия?
2. Перечислите основные возможности методики совокупной стоимости владения компании *Gartner Group*.

3. Приведите основные статьи прямых расходов на обеспечение информационной безопасности предприятия.
4. Приведите основные статьи косвенных расходов на обеспечение информационной безопасности предприятия.
5. Как рассчитывается эффективность подразделения по защите информации?

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 – *экзамен в 1-м семестре.*

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

1. Понятие и задачи информационной безопасности.
2. Уровни обеспечения информационной безопасности.
3. Правовая защита информации.
4. Место информационной безопасности в системе национальной безопасности.
5. Политика обеспечения информационной безопасности Российской Федерации.
6. Современные проблемы информационной безопасности.
7. Модель информационной безопасности организации.
8. Стандартизация процессов управления информационной безопасностью.
9. Состав организационно-распорядительных документов по обеспечению информационной безопасности.
10. Концепция информационной безопасности.
11. Корпоративная политика информационной безопасности.
12. Частные политики информационной безопасности.
13. Система управления информационной безопасностью.
14. Стратегии построения системы управления информационной безопасностью.
15. Процессный подход к управлению информационной безопасностью.
16. Ресурсы, результаты, владельцы процесса управления информационной безопасностью.
17. Программные средства управления информационной безопасностью.
18. Содержание технического задания на создание системы обеспечения информационной безопасности предприятия.
19. Организационные вопросы управления информационной безопасностью.
20. Состав и основные функции службы безопасности организации.
21. Технические аспекты управления информационной безопасностью.
22. Классификация угроз информационной безопасности.
23. Классификация уязвимостей.
24. Классификация информационных рисков.
25. Идентификация и анализ информационных рисков.
26. Методы оценивания информационных рисков.
27. Обеспечение безопасности персональных данных.

28. Аудит информационной безопасности.
29. Экономическая оценка обеспечения информационной безопасности.
30. Методика совокупной стоимости владения компании *Gartner Group*
31. Измерение информационной безопасности.
32. Модели зрелости процессов управления информационной безопасностью.

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

Провести расчет информационных рисков на основе данных таблицы, приведенной ниже:
1) рассчитать общий уровень угроз по ресурсу;
2) Определить общий риск по ресурсу.

Критерий критичности для программно-аппаратной защиты – 30 000 руб.
Критерий критичности для организационной защиты – 40 000 руб.
Критерий критичности для инженерно-технической защиты – 1000 000 руб.

За-щи-та	Угроза	Уязвимость	Вероятность реализации, %	Критич-ность, %
Программно-аппаратная	Несанкционированный доступ к информации, хранящейся на сервере	Хранение данных на сервере в незашифрованном виде	50	70
		Отсутствие межсетевых экранов	30	50
	Потеря информации из-за вирусов и шпионских программ	Отсутствие постоянно обновляемого антивирусного программного обеспечения, межсетевого экрана	60	40
		Использование нелицензионного программного обеспечения	50	40
		Отсутствие ограничения доступа к внешней сети	10	30
	Несанкционированный доступ к информации, хранящейся на АРМ	Недостаточность системы аутентификации пользователей	40	60
		Отсутствие средств защиты от несанкционированного доступа по сети	50	50
Организационная	Физический доступ нарушителя к документам	Недостатки в организации контрольно-пропускного режима на предприятии	70	80
		Отсутствие видеонаблюдения	40	60
	Разглашение конфиденциальной информации	Отсутствие соглашения о неразглашении конфиденциальной информации	30	30
		Нечеткое распределение ответственности за документы между сотрудниками предприятия	70	50
	Несанкционированное копирование и печать конфиденциальных документов	Нечеткая организация конфиденциального документооборота	70	50
		Неконтролируемый доступ сотрудников к копировальной технике	70	50
Инженерно-	Съем информации за счет ПЭМИН	Отсутствие генераторов зашумления, экранирования	10	30
		Превышение уровня опасного сигнала за пределами контролируемой зоны	15	40
	Съем информации с телефонной линии	Отсутствие устройств контроля напряжения телефонной линии	30	40

		Не проводятся специальные обследования и проверки при установке нового оборудования, а также при проведении совещаний	20	40
	Пожар	Уязвимости в системе противопожарной сигнализации, истечение срока эксплуатации огнетушителей	70	90
		Отсутствие несгораемого сейфа	20	60

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».

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
«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 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".

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 (презентационный редактор Microsoft Power Point).

При проведении **лабораторных работ** предусматривается использование программного обеспечения Microsoft Office: (текстовый редактор Microsoft Word; электронные таблицы Microsoft Excel), а также свободного программного обеспечения ARIS Express.

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 Аверченков В.И. Служба защиты информации: организация и управление: [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – М.: ФЛИНТА, 2016. – 186 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=93356

2 Гультяева Т.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Т.А. Гультяева; Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2018. – 79 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=574729

3 Шилов А.К. Управление информационной безопасностью [Электронный ресурс]: учебное пособие / А.К. Шилов; Министерство науки и высшего образования РФ, Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2018. – 121 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=500065

Дополнительная литература.

1 Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов / В.И. Аверченков. – М.: ФЛИНТА, 2016. – 269 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=93245

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 Веселов Г.Е. Менеджмент риска информационной безопасности [Электронный ресурс]: учебное пособие / Г.Е. Веселов, Е.С. Абрамов, А.К. Шилов; Министерство образования и науки РФ, Южный федеральный университет, Инженерно-технологическая академия. – Таганрог: Издательство Южного федерального университета, 2016. – 109 с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=493331

Список авторских методических разработок.

1 Булыгина О.В. Методические рекомендации по выполнению лабораторных работ по дисциплине «Управление информационной безопасностью», расположены в ЭИОС филиала и на кафедральных ресурсах в ауд. 210

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 Росстата [электронный ресурс] — Режим доступа: www.gks.ru/

4 20 интернет-ресурсов для специалистов по информационной безопасности // официальный сайт компании «ГЕОЛАЙН Технологии» [электронный ресурс] — Режим доступа: http://geoline-tech.com/top-20-sites-about-information-security/

5 Полезные сайты и инструменты// Информационная безопасность. Практика информационной безопасности [электронный ресурс] — Режим доступа: http://dorlov.blogspot.com/p/blog-page_3151.html

6 Информационная безопасность [электронный ресурс] — Режим доступа: http://www.securrity.ru/

7 30 ресурсов по безопасности, которые точно пригодятся [электронный ресурс] — Режим доступа: https://proglib.io/p/information-security-guide/

8 Информационная безопасность. Защита данных // habr - веб-сайт в формате коллективного блога с элементами новостного сайта [электронный ресурс] — Режим доступа: https://habr.com/ru/hub/infosecurity/

9 База Знаний Клуба Информационной безопасности [электронный ресурс] — Режим доступа: http://wiki.informationsecurity.club/doku.php/main

10 Информационная безопасность. Защита данных [электронный ресурс] — Режим доступа: http://all-ib.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