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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Владелец: Федулов Александр Сергеевич
Сертификат: 5A022291D0DE01CCADCB2B81371C7969
Действителен: 06.05.2025 - 30.07.2026

УТВЕРЖДАЮ
Зам. директора филиала ФГБОУ ВО
«НИУ «МЭИ» в г. Смоленске
канд. техн. наук, доцент
_____ В.В. Рожков
«06» 03 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: 09.03.03 «Прикладная информатика»

Профиль «Безопасность экономических информационных систем»

Уровень высшего образования: бакалавриат

Нормативный срок обучения: 4 года

Форма обучения: очная

Год набора: 2026

Смоленск

Программа составлена с учетом ОС ВО по направлению подготовки 09.03.03 Прикладная информатика, утвержденного ректором ФГБОУ ВО «НИУ «МЭИ» Н.Д. Рогалевым 20.12.2023.

Программу составил:
канд. техн. наук, доц. _____ А.Ю. Пучков
подпись ФИО

«17» февраля 2026 г.

Программа обсуждена и одобрена на заседании кафедры информационных технологий в экономике и управлении
«18» февраля 2026 г., протокол № 6

Заведующий кафедрой информационных технологий в экономике и управлении:

_____ д-р техн. наук, проф. М.И. Дли
подпись ФИО

«05» марта 2026 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

«05» марта 2026 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является подготовка обучающихся к решению задач профессиональной деятельности организационно-управленческого типа в области информационных и коммуникационных технологий по направлению подготовки 09.03.03 Прикладная информатика (профиль подготовки: Безопасность экономических информационных систем) посредством обеспечения этапов формирования компетенций, предусмотренных ОС и установленных программой бакалавриата на основе профессиональных стандартов, в части представленных ниже знаний, умений и навыков.

Задачи дисциплины:

- ознакомить обучающихся со способами определения круг задач для аудита информационной безопасности в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
- сформировать практические навыки выполнять работы и управлять работами по созданию (модификации) и сопровождению информационных систем, обеспечивающих информационную безопасность, автоматизирующих задачи организационного управления и бизнес-процессы информационной безопасности;
- научить внедрять системы защиты информации автоматизированных систем и обеспечить защиту информации в процессе их эксплуатации;
- выработать способности к планированию задач для аудита информационной безопасности в зоне своей ответственности с учетом имеющихся ресурсов и ограничений, действующих правовых норм;
- привить навыки выполнения задач аудита информационной безопасности в зоне своей ответственности в соответствии с запланированными результатами и точками контроля, при необходимости корректирует способы решения задач;
- дать представление о стандартах и технологиях аудита информационной безопасности;
- сформировать практические навыки диагностики систем защиты информации автоматизированных информационных систем;
- сформировать практические навыки мониторинга и аудита защищенности информации в автоматизированных информационных систем;
- сформировать умение устанавливать и настраивать средства защиты информации в автоматизированных информационных системах;
- развить умение подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе в аудите информационной безопасности;
- научить применять системный подход к информатизации и автоматизации решения прикладных задач, к построению информационных систем на основе современных информационно-коммуникационных технологий и математических методов;
- привить умение к аналитической деятельности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина Аудит информационной безопасности относится *к части, формируемой участниками образовательных отношений.*

Для изучения данной дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами*:*

Б1.О.06 Информационные технологии

Б1.О.07 Программные средства для экономико-математических расчетов

Б1.О.08 Учет и анализ

Б1.О.09 Вычислительные системы, сети и телекоммуникации
Б1.О.10 Управление проектами
Б1.О.11 Операционные системы
Б1.О.13 Правоведение
Б1.О.14 Теория систем и системный анализ
Б1.О.15 Алгоритмизация и программирование
Б1.О.16 Базы данных
Б1.О.17 Разработка и стандартизация программных средств и информационных технологий
Б1.В.01 Экономическая информатика
Б1.В.03 Организационные основы информационной безопасности
Б1.В.04 Реинжиниринг и управление бизнес-процессами
Б1.В.05 Менеджмент
Б1.В.06 Предметно-ориентированные экономические информационные системы
Б1.В.07 Маркетинг
Б1.В.ДВ.01.01 Цифровая экономика
Б1.В.ДВ.01.02 Информационная логистика
ФТД.04 Общественный проект «Обучение служением»

Перечень последующих дисциплин и практик, для которых необходимы знания, умения и навыки, формируемые данной дисциплиной:
Б1.В.10 Информационная безопасность веб-приложений
Б1.В.11 Управление инцидентами информационной безопасности организации
Б1.В.12 Основы экономической безопасности бизнеса
Б1.В.14 Информационная безопасность телекоммуникационных систем и сетей связи
Б1.В.15 Проектный практикум
Б1.В.16 Программная инженерия
Б1.В.18 Контроллинг
Б1.В.ДВ.02.01 Управление инновациями и инвестициями
Б1.В.ДВ.02.02 Корпоративные информационные системы
Б1.В.ДВ.03.01 Интеллектуальные информационные системы
Б1.В.ДВ.03.02 Мировые информационные ресурсы
Б1.В.ДВ.04.01 Стратегический анализ и стратегии информационной безопасности
Б1.В.ДВ.04.02 Информационная бизнес-аналитика
Б2.В.02(П) Технологическая (проектно-технологическая) практика
Б2.В.04(Пд) 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 ОС 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-2. Способен определять круг задач в рамках по-	УК-2.3 Планирует реализацию задач в зоне своей ответственности с учетом имеющихся ресурсов и	Знает: способы определения круга задач аудита информационной безопасности в рамках поставленной

ставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	ограничений, действующих правовых норм	цели. Умеет: планировать реализацию задач аудита информационной безопасности в зоне своей ответственности. Владеет: методами планирования и реализации задач аудита информационной безопасности в зоне своей ответственности с учетом имеющихся ресурсов и ограничений, действующих правовых норм.
	УК-2.4 Выполняет задачи в зоне своей ответственности в соответствии с запланированными результатами и точками контроля, при необходимости корректирует способы решения задач	Знает: задачи аудита информационной безопасности в зоне своей ответственности. Умеет: решать задачи аудита информационной безопасности в зоне своей ответственности в соответствии с запланированными результатами и точками контроля. Владеет: методами решения задач аудита информационной безопасности в зоне своей ответственности.
ПК-3. Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-3.4 Обеспечивает соответствие процессов интеграционного тестирования ИС стандартам и технологиям	Знает: стандарты и технологии интеграционного тестирования безопасности ИС. Умеет: обеспечивать соответствия процессов интеграционного тестирования безопасности ИС стандартам и технологиям. Владеет: методами обеспечения соответствия процессов интеграционного тестирования безопасности ИС стандартам и технологиям.
	ПК-3.5 Реализует процесс обеспечения и контроля качества работ, осуществляет мониторинг хода выполнения работ	Знает: процесс обеспечения и контроля качества работ, осуществляет мониторинг хода выполнения аудита информационной безопасности. Умеет: осуществлять мониторинг хода выполнения аудита информационной безопасности. Владеет: методами реализации процесса обеспечения и контроля качества работ, осуществляет мониторинг хода выполнения аудита информационной безопасности.
ПК-6. Способен внедрять системы защиты информации автоматизированных систем и обеспечить	ПК-6.1 Проводит диагностику систем защиты информации автоматизированных информационных систем	Знает: системы защиты информации автоматизированных систем и как обеспечить защиту информации в процессе их эксплуатации. Умеет: проводить диагностику си-

защиту информации в процессе их эксплуатации		стем защиты информации автоматизированных информационных систем Владеет: методами диагностики систем защиты информации автоматизированных информационных систем
	ПК-6.4 Осуществляет мониторинг и аудит защищенности информации в автоматизированных информационных системах	Знает: процесс мониторинга и аудита защищенности информации в автоматизированных информационных системах. Умеет: осуществлять мониторинг и аудит защищенности информации в автоматизированных информационных системах. Владеет: методами мониторинга и аудита защищенности информации в автоматизированных информационных системах.
	ПК-6.5 Устанавливает и настраивает средства защиты информации в автоматизированных информационных системах	Знает: принципы установки и настройки средств защиты информации в автоматизированных информационных системах. Умеет: устанавливать и настраивать средства защиты информации в автоматизированных информационных системах. Владеет: методами установки и настройки средств защиты информации в автоматизированных информационных системах.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Структура дисциплины:

№	Индекс	Наименование	Семестр 5										Семестр 6										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			
6	Б1.В.09	Аудит информационной безопасности	Эк РГР	**180**	68	34	34			76	36	5													Эк РГР	**180**	68	34	34			76	36	5		20	5

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. Понятие, цели, задачи проведения аудита информационной безопасности.* *1.2. Концептуальные основы аудита информационной безопасности.* *1.3. Этапы проведения аудита информационной безопасности.* *1.4. Основные направления деятельности в области аудита информационной безопасности.* *1.5. Классификация мероприятий аудита.* *1.6. Методы анализа данных при аудите информационной безопасности.* *1.7. Предпосылки создания стандартов информационной безопасности.* *1.8. Международные стандарты аудита информационной безопасности.* *1.9. Российские стандарты аудита информационной безопасности.* *1.10. Классификация и сравнение стандартов аудита информационной безопасности.* *1.11. Модели угроз безопасности и уязвимостей информационных ресурсов.* *1.12. Обзор методик проведения аудита информационной безопасности.* *1.13. Методы оценивания информационных рисков организации.* *1.14. Тестирование как один из основных типов аудита* *1.15. Программные продукты, предназначенные для анализа и управления рисками.* *1.16. Программа сертификации Интернет-сайтов и информационных систем.* *1.17. Диагностика систем защиты информации автоматизированных информационных систем.*
2	Лабораторные работы 8 шт. по 4 часа и 1 шт. по 2 часа: *2.1. Оценка уровня безопасности с использованием CVSS (4 часа)* *2.2. Аттестация объектов информатизации по требованиям безопасности (4 часа)* *2.3. Исследование политик информационной безопасности (4 часа)* *2.4. Разработка политики информационной безопасности для организации (4 часа)* *2.5. Разработка модели угроз безопасности и уязвимостей информационных ресурсов организации. (4 часа)* *2.6. Анализ результатов АИБ (регрессионный анализ: парный и множественный). (4 часа)* *2.7. Обработка результатов аудита ИБ в условиях неопределенности данных(4 часа)* *2.8. Применение нейросетевых моделей для анализа результатов АИБ (4 часов)* *2.9. Применение глубоких нейронных сетей для анализа результатов АИБ (2 часа)*
3	Расчетно-графическая работа: «анализа результатов аудита информационной безопасности»
4	Самостоятельная работа студентов: *изучение основных понятий аудита информационной безопасности, целей аудита информационной безопасности, задач аудита информационной безопасности, определений из общих вопросов информационной безопасности, этапы проведения аудита информационной безопасности, основных направлений деятельности в области информационной безопасности, требований аудита информационной безопасности, требований к квалификации аудитора по информационной безопасности, международных стандартов аудита информационной безопасности, российских стандартов аудита информационной безопасности, структуры плана проведения аудита информационной безопасности на основе международных стандартов, моделей угроз безопасности информационных систем, уязвимостей информационных ресурсов, методик проведения аудита информационной безопасности, определений и видов рисков информационной*

	безопасности, программных продуктов, предназначенных для анализа рисков.

Текущий контроль:

Индикаторы достижения компетенции	Вид текущего контроля	Тема
УК-2.4 Выполняет задачи в зоне своей ответственности в соответствии с запланированными результатами и точками контроля, при необходимости корректирует способы решения задач	Тестирование. Защита лабораторной (лабораторных) работы. Проверка конспектов лекций и дополнительных материалов. Проверка выполнения заданий расчетно-графической работы. Проверка отчета по расчетно-графической работе.	Предпосылки создания стандартов информационной безопасности. Международные стандарты аудита информационной безопасности. Российские стандарты аудита информационной безопасности.
ПК-6.5 Устанавливает и настраивает средства защиты информации в автоматизированных информационных системах	Защита лабораторной (лабораторных) работы. Проверка конспектов лекций и дополнительных материалов. Проверка выполнения заданий расчетно-графической работы.	Этапы проведения аудита информационной безопасности. Основные направления деятельности в области аудита информационной безопасности.
ПК-6.1 Проводит диагностику систем защиты информации автоматизированных информационных систем	Защита лабораторной (лабораторных) работ Проверка конспектов лекций и дополнительных материалов Проверка выполнения заданий расчетно-графической работы Проверка отчета по расчетно-графической работе	Программные продукты, предназначенные для анализа и управления рисками. Диагностика систем защиты информации автоматизированных 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)
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: 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.

Оценочные средства текущего контроля

Вопросы по формированию и развитию теоретических знаний, предусмотренных компетенциями, закрепленными за дисциплиной (вопросы для самопроверки, полученных знаний):

1. Понятие аудита информационной безопасности.
2. Цели аудита информационной безопасности.
3. Задачи аудита информационной безопасности.
4. Определения из общих вопросов информационной безопасности.
5. Этапы проведения аудита информационной безопасности.
6. Основные направления деятельности в области информационной безопасности.
7. Требования аудита информационной безопасности.
8. Требования к квалификации аудитора по информационной безопасности.
9. Перечислить международные стандарты аудита информационной безопасности.
10. Перечислить российские стандарты аудита информационной безопасности.
11. Структура плана проведения аудита информационной безопасности на основе международных стандартов.
12. Структура плана проведения аудита информационной безопасности на основе международных стандартов.
13. Модели угроз безопасности информационных систем.
14. Уязвимости информационных ресурсов.
15. Методики проведения аудита информационной безопасности.
16. Сравнительная характеристика методик проведения аудита.
17. Определение и виды рисков информационной безопасности.
18. Перечислить программные продукты, предназначенные для анализа рисков.
19. Структура сертификата информационной безопасности Интернет-сайтов.
20. Назначение и структура имитационных моделей управления рисками информационной безопасности.

Вопросы по приобретению и развитие практических умений, предусмотренных компетенциями, закрепленными за дисциплиной:

1. Разработать этапы проведения аудита информационной безопасности в соответствии с заданным международным стандартом.
2. Разработать этапы проведения аудита информационной безопасности в соответствии с заданным российским стандартом.
3. Оценить источники уязвимостей для предложенной информационной системы.
4. Оценить источники уязвимостей для предложенного сайта 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 – *экзамен в 5-м семестре.*

Оценочные средства промежуточной аттестации

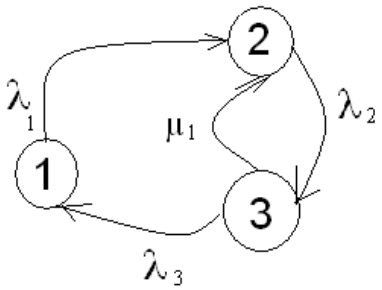
Вопросы по закреплению теоретических знаний, умений и практических навыков, предусмотренных компетенциями (вопросы к экзамену)

1. Аудит информационной безопасности (ИБ): понятие, задачи, цели.
2. Стандарты и практики, применяемые в аудите. Базовые принципы аудита ИБ.
3. Критерии ценности аудит-заключения. Основные этапы ИБ-аудита и их содержание. Документы, создаваемые в результате ИБ-аудита.
4. Направления ИБ-аудита. Возможные результаты проведения ИБ-аудита.
5. Информационные технологии востребованные в современном ИБ-аудите. Помехи ИБ-проектам.
6. Стандарты и методики в области разработки ИБ-аудита.
7. Стандарт ГОСТ Р 50922-2006: назначение, структура, области применения.
8. Стандарты ISO/IEC 17799:2005: назначение, область применения, структура.
9. Иерархическая структура ИБ-аудита.
10. Анализ требований и определение спецификации ИБ-аудита программного обеспечения. Требования к спецификации.
11. Динамическое программирование в задаче обеспечения ИБ.
12. Понятие надежности. Структура ГОСТ 27 – Надежность в технике.
13. Модели надежности в технике.
14. Свойства, характеризующие надежность.
15. Надежности программного обеспечения. Объекты уязвимости программного обеспечения и дестабилизирующие факторы.
16. Обеспечение надежности на различных этапах жизненного цикла вычислительных систем.
17. Сертификация программного обеспечения. Рынок программных средств.
18. Источники угроз для Интернет-ресурсов и пути их нейтрализации.
19. Мероприятия, обеспечивающие приемлемый уровень ИБ.

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

Задача 1.

Граф переходов состояний информационного оборудования организации показан на рисунке. Интенсивности переходов (1/час): $\mu_1 = 0.1$ $\lambda_1 = 0.2$ $\lambda_2 = 0.6$ $\lambda_3 = 0.7$. Рассчитать коэффициент готовности оборудования в установившемся режиме.



Задача 2.

К началу трехлетнего периода в организации приобретена система обеспечения ИБ (про-

граммная и аппаратная часть). Эффективность противодействия атакам на вычислительные средства организации (в денежном эквиваленте), а также зависимость затрат на обновление программ, содержание и ремонт системы обеспечения ИБ при различном времени его использования приведены в таблице 1. Зная, что затраты, связанные с приобретением и установкой новой системы обеспечения ИБ, составляют C = 40 тыс. руб., а заменяемая система списывается, составить такой план замены системы в течении 3 лет, при котором общая прибыль за данный период максимальна.

Таблица 1 – Исходные данные для задачи ДП

	Время t, в течении которого используется оборудование (лет)		
	0	1	2
Эффективность противодействия атакам R(t) в стоимостном выражении (тыс. руб.)	80	75	50
Ежегодные затраты Z(t) на содержание системы ИБ (тыс. руб.)	20	25	35

Задача 3.

Выявить в предложенном для анализа Интернет-ресурсе возможные угрозы для информационной безопасности и предложить возможные направления работ по их нейтрализации.

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».

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
«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 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.

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 Гродзенский Я.С. Информационная безопасность : учебное пособие : [16+] / Я.С. Гродзенский. – Москва : Проспект, 2020. – 142 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=607433

2 Программно-аппаратные средства защиты информации : учебное пособие / Л.Х. Мифтахова, А.Р. Касимова, В.Н. Красильников и др. – Санкт-Петербург : ИЦ "Интермедия", 2018. – 408 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=481123

Дополнительная литература.

1 Рагозин Ю.Н. Инженерно-техническая защита информации : учебное пособие / Ю.Н. Рагозин. – Санкт-Петербург : ИЦ "Интермедия", 2018. – 168 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=481159

2 Скабцов Н. Аудит безопасности информационных систем. – СПб.: Питер, 2018. – 272 с.

3 Гультяева Т.А. Основы информационной безопасности : учебное пособие : [16+] / Т.А. Гультяева ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574729

Список авторских методических разработок.

1 Пучков А.Ю. Методические указания к лабораторной работе «Разработка плана проведения аудита информационной безопасности на основе международных стандартов» по дисциплине «Аудит информационной безопасности» [Электронный ресурс]: электронные методические указания для студентов, обучающихся по направлению 10.04.01 «Информационная безопасность» / Пучков А.Ю. – Электрон. дан. – Смоленск: РИО филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2019

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