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
«28» 08 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

АУДИТ 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: 2021

Смоленск

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

Программу составил:

подпись к.т.н., доцент А.Ю. Пучков
ФИО

«25» июня 2021 г.

Программа обсуждена и одобрена на заседании кафедры «Информационных технологий в экономике и управлении»:
«30» июня 2021 г., протокол № 13

Заведующий кафедрой «Информационных технологий в экономике и управлении»:

подпись д.т.н., профессор М.И. Дли
ФИО

«02» июля 2021 г.

Согласовано:

Заведующий кафедрой «Вычислительной техники»:

подпись д.т.н., профессор А.С. Федулов
ФИО

«02» июля 2021 г.

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Ответственный в филиале по работе
с ЛОВЗ и инвалидами

подпись зам. начальника УУ Е.В. Зуева
ФИО

«02» июля 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 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 предшествующей дисциплиной:

Б1.В.01 Организационно-правовые механизмы обеспечения информационной безопасности
Б1.В.04 Информационная безопасность компьютерных сетей

Б1.В.07 Технические средства защиты информации

Знания, умения и навыки, формируемые данной дисциплиной необходимы для изучения следующих дисциплин, прохождения соответствующих видов практик и прохождения государственной итоговой аттестации:

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: методы и методики оценки безопасности программно-аппаратных средств; методы оценки эффективности политики безопасности, реализованной в программно-аппаратных средствах защиты информации; методы и средства оценки корректности и эффективности программных реализаций алгоритмов защиты информации; методы анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. Умеет: оценивать эффективность защиты информации; анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемой ими защищенности доверия. Владеет: методами оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик; методами определения защищенности и доверия программно-аппаратных средств защиты информации.

	ПК-3.2 Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей	Знает: модели безопасности компьютерных систем; виды политик безопасности компьютерных систем и сетей; национальные, межгосударственные и международные стандарты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти; организационные меры по защите информации. Умеет: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации систем защиты информации; формировать политики безопасности компьютерных систем и сетей. Владеет: методами принятия решений о необходимости защиты информации, содержащейся в информационной системе; методами разработки моделей угроз безопасности информации - методами формирования заданий требований к защите информации компьютерной системы.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Структура дисциплины:

№	Индекс	Наименование	Семестр 3										Семестр 4										Итого за курс										Каф.	Семестр
			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	Контроль				Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Контроль				Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Контроль	Всего			
4	*Б1.В.ДВ.02.02*	*Аудит информационной безопасности*	ЗаО РГР	**144**	86	34	34	18		40	18	4													ЗаО РГР	**144**	86	34	34	18		40	18	4		20	3

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: Тема 1. Понятие, цели, задачи, мероприятия аудита информационной безопасности 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. Тема 2. Стандарты аудита 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. Тема 3. Методы обработки данных 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 2.2. Аттестация объектов информатизации по требованиям безопасности 2.3. Исследование политик информационной безопасности 2.4. Разработка политики информационной безопасности для организации 2.5. Разработка модели угроз безопасности и уязвимостей информационных ресурсов организации 2.6. Анализ результатов АИБ (регрессионный анализ: парный и множественный) 2.7. Обработка результатов аудита ИБ в условиях неопределенности данных 2.8. Применение нейросетевых моделей для анализа результатов АИБ 2.9. Применение глубоких нейронных сетей для анализа результатов АИБ (2 часа)
3	Практические занятия 9 шт. по 2 часа: 3.1. Методика проведения аудита информационной безопасности в организации. 3.2. Составление плана аудита ИБ. 3.3. Проведение аудита ИБ в соответствие со стандартом ISO 15408. 3.4. Проведение аудита ИБ в соответствие со стандартом ISO 17799 3.5. Оценка последствий несанкционированного доступа к информационным ресурсам. 3.6. Анализ существующих подходов оценки рисков ИБ. Методика Microsoft. 3.7. Оценки рисков ИБ. Метод CRAMM. Методика RiskWatch. 3.8. Методики оценки рисков ИБ: FRAP и OCTAVE. 3.9. Интеллектуальный анализ рисков ИБ
4	Расчетно-графическая работа «Анализ результатов аудита информационной безопасности»
5	Самостоятельная работа студентов:

	5.1 Понятие, цели, задачи, мероприятия аудита информационной безопасности. 5.2 Стандарты аудита информационной безопасности. 5.3 Методы обработки данных аудита информационной безопасности. 5.4 Самостоятельная работа по выполнению РГР

Текущий контроль:

Индикаторы достижения компетенции	**Вид текущего контроля**	**Тема**
ПК-3.1 Проводит анализ безопасности компьютерных систем и сетей	Собеседование Опрос Разбор конкретных ситуаций и групповые дискуссии по темам практических занятий Защита лабораторных работ	Тема 1. Понятие, цели, задачи, мероприятия аудита информационной безопасности Тема 2. Стандарты аудита информационной безопасности
ПК-3.2 Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей	Собеседование Опрос Разбор конкретных ситуаций и групповые дискуссии по темам практических занятий Защита лабораторных работ Проверка выполнения заданий расчетно-графической работы Проверка отчета по расчетно-графической работе	Тема 2. Стандарты аудита информационной безопасности Тема 3. Методы обработки данных аудита информационной безопасности

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

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

№ п/п	Виды учебных занятий	Образовательные технологии
1	Лекции	Мультимедийное чтение лекций (интерактивная лекция, лекция-визуализация) Индивидуальные и групповые консультации по дисциплине
2	Практические занятия	Технология обучения на основе решения задач и выполнения упражнений. Технологии проведения практических занятий в форме семинара: тематический семинар, проблемный семинар, семинар с подготовленными докладами.
3	Лабораторная работа	Технология выполнения лабораторных заданий индивидуально. Технология выполнения лабораторных заданий в малой группе (в бригаде).
4	Самостоятельная работа студентов (внеаудиторная)	Информационно-коммуникационные технологии (доступ к ЭИОС филиала, к ЭБС филиала, доступ к информационно-методическим материалам по дисциплине)
5	Контроль (промежуточная аттестация: зачет)	Технология устного опроса. Выполнение контрольных заданий на компьютере в заданной программной среде.

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 промежуточного контроля:

Вопросы для защиты лабораторной работы
«Оценка уровня безопасности с использованием CVSS»

1. Понятие информационной безопасности.
2. Цели аудита информационной безопасности.
3. Задачи аудита информационной безопасности.
4. Метрики CVSS.
5. Этапы проведения аудита информационной безопасности

Вопросы для защиты лабораторной работы
«Аттестация объектов информатизации по требованиям безопасности»

1. Цели аттестация объектов информатизации по требованиям безопасности.
2. Стандарты аттестация объектов информатизации по требованиям безопасности
3. Методы аттестация ИБ.
4. Этапы аттестация объектов ИБ.
5. Программные средства, применяемые для аттестации объектов ИБ.

Вопросы для защиты лабораторной работы
«Исследование политик информационной безопасности»

1.Что в себя включает политика ИБ?
2. Стандарты, используемые при разработке политики ИБ.
3. В каком отечественном стандарте прописаны зоны ответственности руководства?
4. Принципы формирования политики информационной безопасности в организации.
5. Основные требования к политике информационной безопасности.

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

1. Какие существуют системы оценки текущей ситуации в области ИБ на предприятии?
2. Какие основные направления разработки ПИБ?
3. Назовите основные этапы разработки ПИБ.
4. Что подразумевает понятие «Политика информационной безопасности»?
5. Какие типы документов включает пакет организационно-распорядительных документов по вопросам обеспечения ИБ.

Вопросы для защиты лабораторной работы
«Разработка модели угроз безопасности и уязвимостей информационных ресурсов организации»

1. Что включает в себя модель угроз безопасности и уязвимостей информационных

ресурсов организации?

2. Назовите основные методы реализации угроз информационной безопасности.
3. Что подразумевает понятие «Угроза нарушения доступности»?
4. Приведите пример классифицирования угроз.
5. Каковы основные направления реализации информационных угроз?

Вопросы для защиты лабораторной работы «Анализ результатов АИБ (регрессионный анализ: парный и множественный)»

1. На каком этапе проведения АИБ осуществляется анализ результатов?
2. Методы, применяемые при анализе результатов АИБ.
3. Назовите этапы построения модели.
4. Какая характеристика используется для оценки тесноты связи между двумя факто-рами (явлениями)?
5. Недостатки корреляционного анализа при поведении анализа результатов АИБ?

Вопросы для защиты лабораторной работы «Обработка результатов аудита ИБ в условиях неопределенности данных»

1. Что понимается под неопределенностью данных?
2. Методы учета неопределенности в данных
3. Какие способы существуют для заполнения пропущенных значений в таблиуах данных?
4. Что такое шкалирование данных?
5. Какие методы искусственного интеллекта позволяют работать с данными в условиях неопределенности?

Вопросы для защиты лабораторной работы «Применение нейросетевых моделей для анализа результатов АИБ»

1. Назовите виды искусственных нейронных сетей.
2. Чему равна размерность входных и выходных данных нейронной сети при анализе влияния пяти параметров на уровень информационной безопасности в организации?
3. Какие основные принципы лежат при формировании обучающей выборки?
4. Возможно ли применение сверточных нейронных сетей для анализа временных рядов?
5. Какие методы позволяют минимизироват набор признаков для обучения нейронных сетей без потери точности ее работы?

Вопросы для защиты лабораторной работы «Применение глубоких нейронных сетей для анализа результатов АИБ»

1. Назовите основные характеристики больших данных.
2. Какие методы входят в аппарат машинного обучения?
3. Что называется глубокой нейронной сетью?
4. Что значит «построение иерархии признаков» нейронной сетью?
5. В чем преимущества глубоких нейронных сетей при их использовании для анализа результатов АИБ?

Вопросы для опроса или собеседования на практических занятиях

Практическое занятие «Методика проведения аудита информационной безопасности в организации»

1. Какие методики проведения аудита информационной безопасности в организации существуют?
2. Какие особенности информационной структуры организации в наибольшей степени

влияют на выбор методики оценки ИБ?

Практическое занятие «Составление плана аудита ИБ»

1. Назначение плана аудита ИБ.
2. Рекомендации по составлению плана АИБ.
3. Стандарты, регламентирующие пункты плана АИБ.

Практическое занятие «Проведение аудита ИБ в соответствие со стандартом ISO 15408»

1. Какие цели реализует стандартом ISO 15408 в области ИБ?
2. Какие требования по анализу уязвимостей и механизмов защиты включает класс под названием AVA: Vulnerability Assessment.
3. Назовите несколько основных отличительных черт «Общих критериев», обозначенных в стандарте.

Практическое занятие «Проведение аудита ИБ в соответствие со стандартом ISO 17799»

1. Какой российский стандарт выполнен на основе ISO 17799?
2. Какие ключевые меры контроля ИБ определены с точки зрения законодательства?
3. Что включают в себя мероприятия по управлению информационной безопасностью?

Практическое занятие «Оценка последствий несанкционированного доступа к информационным ресурсам»

1. Назовите принципы информационной безопасности.
2. Классификация уязвимостей систем безопасности.
3. Назовите методы оценки последствий несанкционированного доступа к информационным ресурсам

Практическое занятие «Анализ существующих подходов оценки рисков ИБ. Методика Microsoft»

1. Что такое риск ИБ и как он измеряется?
2. Методы идентификации рисков ИБ.
3. Этапы проведения количественной оценки рисков.

Практическое занятие «Оценки рисков ИБ. Метод CRAMM. Методика RiskWatch»

1. Качественный и количественный метод оценки рисков ИБ: достоинства и недостатки.
2. Целью применении метода CRAMM.
3. Критерии оценки ценности ресурсов в методе CRAMM

Практическое занятие «Методики оценки рисков ИБ: FRAP и OCTAVE»

1. Какие шкалы применяются для оценки вероятности возникновения угрозы и ущерба ИБ в FRAP.
2. Как строится матрица рисков FRAP?
3. Что включается в затраты при оценке экономической эффективности внедрения средств защиты ИБ?

Практическое занятие «Интеллектуальный анализ рисков ИБ»

1. В чем преимущества применения методов искусственного интеллекта при анализе ИБ?
2. В каких случаях целесообразно применять интеллектуальны методы анализа рисков ИБ?
3. Порядок применения искусственных нейронных сетей для анализа уровня состояния ИБ ворганизации.

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.

Оценочные средства промежуточной аттестации:

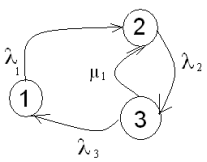
Вопросы по закреплению теоретических знаний, умений и практических навыков, предусмотренных компетенциями (вопросы к зачету)

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.

Пример практических заданий, выносимых на зачет, 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 (программная 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 С = 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.

Форма промежуточной аттестации по настоящей дисциплине – *зачет с оценкой в 3-м семестре.*

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

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
	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 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, демонстрационным оборудованием: персональным компьютером (ноутбуком); переносным (стационарным).

Для проведения практических занятий

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

- специализированной мебелью; доской аудиторной.

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 (презентационный редактор Microsoft Power Point).

При проведении лабораторных работ предусматривается использование программного обеспечения Microsoft Office: (текстовый редактор Microsoft Word; электронные таблицы Microsoft Excel), MatLab.

Для выполнения расчетно-графической работы предусматривается использование обучающимися программного обеспечения Microsoft Office: (текстовый редактор Microsoft Word; электронные таблицы Microsoft Excel), MatLab.

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