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

СТРАТЕГИЧЕСКИЙ АНАЛИЗ И СТРАТЕГИИ 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:
д-р. экон. наук, проф. _____ Л.В. Фомченкова
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 и проектного типов 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 с сущностью и основными концепциями стратегического управления информационной безопасностью; методами стратегического анализа внешних и внутренних условий информационной безопасности организации; структурой информации, необходимой для проведения стратегического анализа; типологией стратегий информационной безопасности организации; процессом их реализации; ролью информационных и операционных систем в обеспечении эффективности стратегического управления информационной безопасностью; факторами и показателями оценки эффективности стратегии информационной безопасности;
- сформировать умения формировать стратегические цели организации; идентифицировать факторы, влияющие на выбор стратегии информационной безопасности организации; формировать информационное обеспечение стратегического анализа; оценивать внешние факторы при разработке стратегии информационной безопасности организации; использовать информационные системы для сбора информации, необходимой для стратегического анализа; разрабатывать корпоративные, конкурентные и функциональные стратегии развития организации; осуществлять выбор стратегии информационной безопасности организации; адаптировать организационную структуру организации к реализуемым стратегиям с учетом информационной безопасности; оценивать риски реализации стратегии организации;
- выработать практические навыки стратегического целеполагания; стратегического анализа деловой среды организации, ее бизнес-модели, бизнес-процессов и ресурсов; обработки деловой информации, необходимой для проведения стратегического анализа; разработки стратегий организации; обоснования стратегии информационной безопасности организации; моделирования системы стратегического управления информационной безопасностью организации; стратегического контроля информационной безопасности организации; оценки эффективности стратегий.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина Стратегический анализ и стратегии информационной безопасности относится *к части, формируемой участниками образовательных отношений.*

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

Б1.О.03 Философия
Б1.О.10 Управление проектами
Б1.О.14 Теория систем и системный анализ
Б1.В.01 Экономическая информатика
Б1.В.02 Экономическая статистика
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.08 Финансовый менеджмент
Б1.В.09 Аудит информационной безопасности
Б1.В.10 Информационная безопасность веб-приложений
Б1.В.11 Управление инцидентами информационной безопасности организации
Б1.В.12 Основы экономической безопасности бизнеса
Б1.В.13 Проектирование информационных систем
Б1.В.ДВ.01.01 Цифровая экономика
Б1.В.ДВ.01.02 Информационная логистика
Б1.В.ДВ.02.01 Управление инновациями и инвестициями
Б1.В.ДВ.02.02 Корпоративные информационные системы
Б2.В.01(У) Ознакомительная практика
Б2.В.02(П) Технологическая (проектно-технологическая) практика
ФТД.04 Общественный проект «Обучение служением»

Перечень последующих дисциплин и практик, для которых необходимы знания, умения и навыки, формируемые данной дисциплиной:
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.03.01 Интеллектуальные информационные системы
Б1.В.ДВ.03.02 Мировые информационные ресурсы
Б2.В.03(Н) Научно-исследовательская работа
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-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Анализирует задачу, выделяя ее базовые составляющие	Знает: сущность стратегического анализа внешних и внутренних условий информационной безопасности организации Умеет: идентифицировать факторы, влияющие на выбор стратегии информационной безопасности организации Владеет: навыками стратегического анализа деловой среды организации
	УК-1.2 Определяет, интерпретирует и ранжирует информацию, требуемую для	Знает: структуру информации, необходимую для проведения стратегического анализа Умеет: формировать информационное обеспе-

Компетенция	Индикаторы достижения компетенций	Результаты обучения
	решения поставленной задачи	чение стратегического анализа Владеет: навыками обработки деловой информации, необходимой для проведения стратегического анализа
	УК-1.3 Осуществляет поиск информации для решения поставленной задачи по различным типам запросов	Знает: основные концепции стратегического управления информационной безопасностью Умеет: оценивать внешние факторы при разработке стратегии информационной безопасности организации Владеет: навыками стратегического анализа бизнес-модели, бизнес-процессов и ресурсов организации
	УК-1.4 При обработке информации отличает факты от мнений, интерпретаций, оценок, формирует собственные мнения и суждения, аргументирует свои выводы и точку зрения	Знает: сущность стратегического управления информационной безопасностью объектов Умеет: разрабатывать корпоративные, конкурентные и функциональные стратегии развития организации Владеет: навыками обоснования стратегии информационной безопасности организации
	УК-1.5 Рассматривает и предлагает возможные варианты решения поставленной задачи, оценивая их достоинства и недостатки	Знает: типологию стратегий информационной безопасности организации Умеет: осуществлять выбор стратегии информационной безопасности организации Владеет: навыками разработки стратегий организации
ПК-2. Способен проводить концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности	ПК-2.2 Анализирует проблемные ситуации заинтересованных лиц, которые могут быть устранены за счет автоматизации	Знает: факторы эффективности стратегии информационной безопасности организации Умеет: оценивать риски реализации стратегии организации Владеет: навыками стратегического целеполагания
	ПК-2.3 Проводит обследование объекта автоматизации, описывает его целевое состояние, определяет значимые показатели деятельности объекта автоматизации, на изменение которых направлен проект, а также устанавливает целевые значения показателей	Знает: роль информационных и операционных систем в обеспечении эффективности стратегического управления информационной безопасностью Умеет: использовать информационные системы для сбора информации, необходимой для стратегического анализа Владеет: навыками моделирования системы стратегического управления информационной безопасностью организации

Компетенция	Индикаторы достижения компетенций	Результаты обучения
ПК-3. Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-3.1 Планирует коммуникации с заказчиком в проектах, представляет результаты о ходе выполнения работ	Знает: процесс реализации стратегии информационной безопасности Умеет: адаптировать организационную структуру организации к реализуемым стратегиям с учетом информационной безопасности Владеет: навыками оценки эффективности стратегий организации
ПК-6. Способен внедрять системы защиты информации автоматизированных систем и обеспечить защиту информации в процессе их эксплуатации	ПК-6.1 Проводит диагностику систем защиты информации автоматизированных информационных систем	Знает: показатели оценки эффективности стратегического управления информационной безопасностью объектов Умеет: формировать стратегические цели организации Владеет: навыками стратегического контроля информационной безопасности организации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Структура дисциплины:

№	Индекс	Наименование	Семестр 7										Семестр 8										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 акт.	Лек	Лаб	Пр	КРП	СР	Конт роль				Всего	Конт акт.	Лек	Лаб	Пр	КРП	СР	Конт роль				Всего	Конт акт.	Лек	Лаб	Пр	КРП	СР	Конт роль	Всего			
9	Б1.В.ДВ.04.01	Стратегический анализ и стратегии информационной безопасности	Экз	180	68	34		34		76	36	5													Экз	180	68	34		34		76	36	5		20	7

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. Сущность стратегического управления информационной безопасностью* *1.2. Понятие и сущность IT-стратегии и стратегии информационной безопасности организации* *1.3. Бизнес-стратегия и стратегия информационной безопасности* *1.4. Процесс разработки стратегии информационной безопасности* *1.5. Процесс стратегического анализа объектов информационной безопасности* *1.6. Методы стратегического анализа* *1.7. Аналитические инструменты разработки стратегии* *1.8. Информационное обеспечение стратегического анализа* *1.9. Типология и процесс выбор стратегии информационной безопасности* *1.10. Модели разработки бизнес-ориентированных стратегий информационной безопасности* *1.11. Ресурсное обеспечение стратегии информационной безопасности* *1.12. Стратегия и политика информационной безопасности организации* *1.13. Процесс реализация стратегии информационной безопасности организации* *1.14. Анализ рисков реализации стратегии информационной безопасности* *1.15. Инвестиционное обеспечение реализации стратегии информационной безопасности* *1.16. Эффективность стратегии информационной безопасности организации* *1.17. Стратегический контроль информационной безопасности*
2	*Практические занятия 17 шт. по 2 часа:* *2.1. Стратегия в системе управления информационной безопасностью* *2.2. Типология стратегий организации* *2.3. Стратегическое целеполагание* *2.4. Методы и инструменты стратегического анализа внешней среды* *2.5. Методы и инструменты стратегического анализа организации* *2.6. Стратегический анализ информационной безопасности* *2.7. Согласование стратегий в организации* *2.8. Политика информационной безопасности в системе стратегического управления организацией* *2.9. Жизненный цикл стратегии информационной безопасности* *2.10. Создание организационных возможностей реализации стратегии* *2.11. Структуры управления организацией и контроля информационной безопасности* *2.12. Техническое обслуживание стратегии информационной безопасности* *2.13. Система стратегического контроля информационной безопасности организации* *2.14. Мониторинг и оценка стратегии информационной безопасности* *2.15. Факторы эффективности стратегии информационной безопасностью* *2.16. Эффективность структуры управления информационной безопасностью* *2.17. Система показателей эффективности стратегического управления информационной безопасностью объектов*
3	Самостоятельная работа студентов: *3.1. Геополитическая стратегия России в сфере информационной безопасности*: основы национальной стратеги России; стратегические цели и основные направления обеспечения информационной безопасности; мировое соотношение информационных технологий в сфере информационной безопасности; системы международной и региональной безопас-

	ности; международное сотрудничество РФ в области обеспечения информационной безопасности *3.2. Методы современного стратегического анализа*: оценка конкурентоспособности продукта (услуги); разработка стратегии на основе SWOT-анализа; анализ жизненного цикла продукта; анализ портфеля бизнесов; стратегический анализ организационной культуры.

Текущий контроль:

- опрос;
- проверка конспектов лекций и дополнительных материалов

Индикаторы достижения компетенции	Вид текущего контроля	Тема
УК-1.1 Анализирует задачу, выделяя ее базовые составляющие	опрос; проверка конспектов лекций и дополнительных материалов	*1.1. Сущность стратегического управления информационной безопасностью* *1.5. Процесс стратегического анализа объектов информационной безопасности* *2.6. Стратегический анализ информационной безопасности* *2.15. Факторы эффективности стратегии информационной безопасностью* *3.2. Методы современного стратегического анализа*
УК-1.2 Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи	опрос; проверка конспектов лекций и дополнительных материалов	*1.7. Аналитические инструменты разработки стратегии* *1.8. Информационное обеспечение стратегического анализа* *2.1. Стратегия в системе управления информационной безопасностью* *3.1. Геополитическая стратегия России в сфере информационной безопасности*
УК-1.3 Осуществляет поиск информации для решения поставленной задачи по различным типам запросов	опрос; проверка конспектов лекций и дополнительных материалов	*1.6. Методы стратегического анализа* *2.4. Методы и инструменты стратегического анализа внешней среды* *2.5. Методы и инструменты стратегического анализа организации* *3.2. Методы современного стратегического анализа*
УК-1.4 При обработке информации отличает факты от мнений, интерпретаций, оценок, формирует собственные мнения и суждения, аргументирует свои выводы и точку зрения	опрос; проверка конспектов лекций и дополнительных материалов	*1.2. Понятие и сущность IT-стратегии и стратегии информационной безопасности организации* *1.4. Процесс разработки стратегии информационной безопасности* *2.2. Типология стратегий организации* *2.7. Согласование стратегий в организации*
УК-1.5 Рассматривает и предлагает возможные варианты решения поставленной задачи, оценивая их достоинства и не-	опрос; проверка конспектов лекций и дополнительных ма-	*1.3. Бизнес-стратегия и стратегия информационной безопасности* *1.9. Типология и процесс выбор стратегии информационной безопасности*

Индикаторы достижения компетенции	Вид текущего контроля	Тема
достатки	териалов	*2.9. Жизненный цикл стратегии информационной безопасности*
ПК-2.2 Анализирует проблемные ситуации заинтересованных лиц, которые могут быть устранены за счет автоматизации	опрос; проверка конспектов лекций и дополнительных материалов	*1.14. Анализ рисков реализации стратегии информационной безопасности* *1.16. Эффективность стратегии информационной безопасности организации* *2.3. Стратегическое целеполагание* *2.14. Мониторинг и оценка стратегии информационной безопасности*
ПК-2.3 Проводит обследование объекта автоматизации, описывает его целевое состояние, определяет значимые показатели деятельности объекта автоматизации, на изменение которых направлен проект, а также устанавливает целевые значения показателей	опрос; проверка конспектов лекций и дополнительных материалов	*1.10. Модели разработки бизнес-ориентированных стратегий информационной безопасности* *1.11. Ресурсное обеспечение стратегии информационной безопасности* *2.10. Создание организационных возможностей реализации стратегии* *2.11. Структуры управления организацией и контроля информационной безопасности* *2.12. Техническое обслуживание стратегии информационной безопасности*
ПК-3.1 Планирует коммуникации с заказчиком в проектах, представляет результаты о ходе выполнения работ	опрос; проверка конспектов лекций и дополнительных материалов	*1.12. Стратегия и политика информационной безопасности организации* *1.13. Процесс реализация стратегии информационной безопасности организации* *2.16. Эффективность структуры управления информационной безопасностью* *2.17. Система показателей эффективности стратегического управления информационной безопасностью объектов*
ПК-6.1 Проводит диагностику систем защиты информации автоматизированных информационных систем	опрос; проверка конспектов лекций и дополнительных материалов	*1.15. Инвестиционное обеспечение реализации стратегии информационной безопасности* *1.17. Стратегический контроль информационной безопасности* *2.8. Политика информационной безопасности в системе стратегического управления организацией* *2.13. Система стратегического контроля информационной безопасности организации*

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	Практические занятия	Технологии проведения практических занятий в форме семинара: тематический семинар, проблемный семинар Технология обучения в сотрудничестве (командная, групповая работа)
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 для опроса на практических занятиях

Практическое занятие «*Стратегия в системе управления информационной безопасностью*»

1. В чем сущность стратегического управления информационной безопасностью организацией? Чем оно отличается от других систем управления организациями?
2. Сколько уровней стратегических решений выделяется на многопрофильных организациях?
3. В чем принципиальное отличие ресурсной концепции стратегического управления от рыночной?
4. Какова взаимосвязь стратегии информационной безопасности с другими стратегиями организации?
5. Каковы особенности управленческих задач высшего руководства организации в сфере информационной безопасности?
6. В чем состоят особенности моделей корпоративного стратегического анализа и планирования?

7. Что понимается под стратегией информационной безопасности организации?

Контрольные вопросы для обсуждения на практическом занятии по теме «*Типология стратегий организации*»:

1. Сущность стратегического управления информационной безопасностью организацией.
2. Взаимосвязь стратегии информационной безопасности с другими стратегиями организации.
3. Стратегия и политика информационной безопасности организации.

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

Форма промежуточной аттестации по настоящей дисциплине – *экзамен в 7-м семестре.*

Оценочные средства промежуточной аттестации

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

1. Предпосылки развития стратегического управления организацией.
2. Сущность стратегического управления информационной безопасностью организацией.
3. Концепция стратегического управления информационной безопасностью.
4. Характеристика современных условий бизнеса. Перспективы развития стратегического управления информационной безопасностью организацией.
5. Преимущества и проблемы стратегического управления информационной безопасностью организацией.
6. Основные задачи стратегического управления информационной безопасностью организацией.
7. Пирамида стратегий организации.
8. Корпоративная стратегия организации. Деловая стратегия организации. Функциональные стратегии. IT-стратегия.
9. Модели стратегического управления организацией.
10. Многоуровневое стратегическое управление организацией.
11. Процесс стратегического управления. Характеристика этапов.
12. Сущность стратегического планирования информационной безопасности.
13. Роль и задачи специалистов по стратегическому управлению информационной безопасностью.
14. Основные направления стратегического анализа.
15. Анализ внешней среды организации как составляющая процесса стратегического анализа.
16. Анализ общей ситуации в отрасли как составляющая процесса стратегического анализа.
17. Стратегический анализ организации.
18. Назначение и сущность портфельного анализа IT-проектов организации.
19. Выбор стратегии информационной безопасности организации.
20. Характеристика стратегий информационной безопасности.
21. Стратегия и политика информационной безопасности.
22. Приведение организационной структуры в соответствие со стратегией.
23. Стратегические преимущества и недостатки различных структур управления организациями.
24. Планирование реализации стратегии информационной безопасности.
25. Создание поддерживающих стратегию политик и процедур.
26. Культура организации: связь со стратегией.
27. Разработка систем стимулирования, поддерживающих стратегию.

28. Оценка эффективности реализации стратегии. Концепция сбалансированной системы показателей.

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

Сравните варианты предложенных организационных структур управления производственной организацией с точки зрения эффективной реализации стратегии информационной безопасности.

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

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

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

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
чтено	нительные 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 практических занятий

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

- специализированной мебелью; доской аудиторной.

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 Данилин А.В. ИТ-стратегия / А.В. Данилин, А.И. Слюсаренко [Электронный ресурс]. — 2-е изд., испр. — Москва : Национальный Открытый Университет «ИНТУИТ», 2016. — 232 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=428980.

2 Стратегическое управление : учебник / И.К. Ларионов, А.Н. Герасин, О.Н. Герасина и др. ; под ред. И.К. Ларионова. – 3-е изд. – Москва : Дашков и К°, 2019. – 235 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=496214 – Текст : электронный.

Дополнительная литература

1 Петренко В.И. Теоретические основы защиты информации [Электронный ресурс] : учебное пособие. — Ставрополь : СКФУ, 2015. — 222 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=458204

2 Калянов Г.Н. Консалтинг: от бизнес-стратегии к корпоративной информационно-управляющей системе [Электронный ресурс] : учебник. — Москва : Горячая линия-Телеком, 2016. — 210 с. — Режим доступа: https://e.lanbook.com/book/94627.

3 Ищейнов В.Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В.Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 – Текст : электронный.

4 Ополченова, Е.В. Современный стратегический анализ : учебное пособие / Е.В. Ополченова ; Российская международная академия туризма. – Москва : Университетская книга, 2016. – 112 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=575004 – Текст : электронный.

Список авторских методических разработок

1 Фомченкова Л.В. Методы стратегического анализа и выбора стратегии организации : методические указания к практическим занятиям по дисциплинам "Информационная бизнес-аналитика", "Стратегический анализ и стратегии информационной безопасности", "Стратегический анализ", "Финансовая стратегия и политика" : по направлениям 09.03.03 "Прикладная информатика" (профиль Безопасность экономических информационных систем) и 38.03.01 "Экономика" (профиль Прикладная экономика, финансы и бухгалтерский учет) / Л.В. Фомченкова ; Министерство науки и высшего образования Российской Федерации, Филиал ФГБОУ ВО "НИУ "МЭИ" в г. Смоленске, Кафедра Информационных технологий в экономике и управлении .— Смоленск : [б. и.], 2021 .— 28 с. : табл. ; 1 файл: 422 Кб .— Загл. с титул. экрана .— Библиогр.: с. 28 .— Системные требования: Acrobat Reader .— Электрон. копия представлена на сайте Библиотеки вуза .— б.ц. — <URL:http://lib.sbmpei.ru/file/upload/L_65.pdf>

2 Методическое обеспечение по дисциплине включает следующие авторские разработки:

– комплект лекций в формате мультимедийных презентаций;

– комплект заданий к практическим занятиям.

Методическое обеспечение размещено в файловом хранилище на кафедральном компьютере в аудитории 210.

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