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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(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. _____ Б.В. Окунев
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 с современными угрозами в ИТ-сфере;
- ознакомить с нормативно-правовыми документами в сфере информационной безопасности;
- выработать способности безопасного коммуницирования с заказчиком;
- сформировать умения сбора и анализа информации для формализации требований заказчика по обеспечению защиты информационных ресурсов;
- развить навыки выбора и анализа программно-технологических платформ, сервисов и информационных ресурсов информационной системы, обеспечивающих защиту информации;
- развить навыки разработки политики информационной безопасности организации и использования методов и средств обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина Информационная безопасность относится *к части, формируемой участниками образовательных отношений.*

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

Б1.В.06 Предметно-ориентированные экономические информационные системы
Б1.В.12 Основы экономической безопасности бизнеса
Б1.В.13 Проектирование информационных систем
Б1.В.16 Программная инженерия
Б1.В.ДВ.01.01 Цифровая экономика
Б1.В.ДВ.03.01 Интеллектуальные информационные системы

Знания, умения и навыки, формируемые данной дисциплиной, необходимы для прохождения преддипломной практики (Б2.В.04(Пд)) и подготовки к защите и защиты выпускной квалификационной работы (Б3.01).

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
ПК-1. Способен проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе	ПК-1.1 Вырабатывает варианты реализации требований к программному обеспечению и анализирует возможности их реализации	Знает: основные методы анализа требований к ИС по защите информации. Умеет: вырабатывать варианты реализаций требований к ИС по защите информации. Владеет: навыками анализа и реализации требований к ИС по защите информации.
	ПК-1.2 Проектирует структуры данных, базы данных, программные интерфейсы, информационные системы по видам обеспечения	Знает: основные элементы проектирования ИС обеспечивающие защиту информации. Умеет: проектировать структуру данных, программные интерфейсы и ИС обеспечивающие защиту информации. Владеет: навыками проектирования баз данных и ИС, которые обеспечивают защиту информации..
	ПК-1.3 Разрабатывает и адаптирует компоненты, модули прикладного программного обеспечения	Знает: основные методы разработки ИС обеспечивающие защиту информации. Умеет: разрабатывать и адаптировать элементы ИС обеспечивающие защиту информации. Владеет: навыками разработки компонентов прикладных ИС обеспечивающих защиту информации.
ПК-5. Способен управлять работами по созданию (модификации) и сопровождению информационных ресурсов	ПК-5.1 Анализирует и формализует требования к информационным ресурсам, предлагает варианты реализации информационных ресурсов и осуществляет коммуникации с заинтересованными лицами	Знает: основные требования к информационным ресурсам, обеспечивающие информационную безопасность. Умеет: анализировать и формализовать требования к информационным ресурсам обеспечивающим информационную безопасность. Владеет: навыками безопасного коммуницирования с заинтересованными лицами.
	ПК-5.2 Осуществляет администрирование и эксплуатацию аппаратно-программных средств в соответствии с требованиями по защите информации	Знает: основные методы администрирования аппаратно-программных средств, в соответствии с требованиями по защите информации. Умеет: анализировать состояние аппаратно-программных средств в со-

		ответствии с требованиями по защите информации. Владеет: навыками эксплуатации аппаратно-программных средств в соответствии с требованиями по защите информации.

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	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			
5	Б1.В.17	Информационная безопасность											Экз РГР	180	50	20	20	10		94	36	5	Экз РГР	180	50	20	20	10		94	36	5		20	8

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 10 шт. по 2 часа: *1.1. Тема: Международные стандарты информационного обмена. Понятие угрозы. Концепция информационной безопасности. Виды противников (или «нарушителей»).* *1.2. Тема: Основные нормативные руководящие документы, законы РФ и т.п. касающиеся государственной тайны и защиты информации.* *1.3. Тема: Виды возможных нарушений информационных систем. Особенности нарушений информационных систем в конкретных предметных областях.* *1.4. Тема: Основные положения теории информационной безопасности информационных систем.* *1.5. Тема: Защита программного обеспечения, основанная на идентификации пользователя. Защита программного обеспечения, основанная на идентификации ПЭВМ.* *1.6. Тема: Методы криптографии. Защита данных. Шифрование данных и программ. Понятие идеального шифра.* *1.7. Тема: Понятие о вредоносных программах. Виды компьютерных вирусов.* *1.8. Тема: Методы защиты информации в вычислительных сетях. Обеспечение информационной безопасности в глобальной сети Интернет.* *1.9. Тема: Использование защищенных компьютерных систем. Организация комплексной защиты.* *1.10. Тема: Таксономия нарушений информационной безопасности вычислительной системы и причины, обусловливающие их существование.*
2	Лабораторные работы 5 шт. по 4 часа: *2.1. Защита от несанкционированного использования программ, основанная на привязке программного обеспечения к аппаратным средствам конкретного компьютера и использовании электронного ключа.* *2.2. Изучение и использование различных методов криптографии для защиты данных. Ассиметричные криптоалоритмы.* *2.3. Изучение и использование различных методов криптографии для защиты данных. Симметричные криптоалоритмы.* *2.4. Организация комплексной защиты информационной инфраструктуры организации. Критическая информационная инфраструктура организаций. Защита от несанкционированного доступа к информационным ресурсам. (Часть1.)* *2.5. Организация комплексной защиты информационной инфраструктуры организации. Критическая информационная инфраструктура организаций. Обнаружение вторжений в информационную инфраструктуру организации. (Часть2.)*
3	Практические занятия 5 шт. по 2 часа: *3.1. Нормативная и законодательная база РФ, обеспечивающая функционирование систем защиты информации.* *3.2. Изучение программных средств, обеспечивающих защиту от вредоносных программ.* *3.3. Основы аудита информационной безопасности. Общая система оценки уязвимостей.* *3.4. Информационные системы персональных данных. Организация и ведение работ по обеспечению безопасности персональных данных при их обработке в информационных системах ПнД.* *3.5. Основные принципы защищенного электронного документооборота. Электронная цифровая подпись.*

4	Расчетно-графическая работа. *Разработка политики информационной безопасности (ПИБ) организации для заданной профессиональной области. Программная реализации криптографического метода защиты (ассиметричный алгоритм RSA).*
5	Самостоятельная работа студентов: *1.1. Тема: Угрозы безопасности персональных данных, уязвимости информационных систем ПнД.* *1.2. Тема: Базовая модель угроз безопасности ПнД.* *1.3.Тема: Организация физическим лицом защиты своих персональных данных.* *1.4. Тема: Виды, источники и классификация угроз информационной безопасности.* *1.5. Тема: Актуальный банк данных угроз информационной безопасности.* *1.6. Тема: Системы обнаружения вторжений.* *1.7. Тема: Аудит информационной безопасности.* *1.8. Тема: Частные виртуальные сети.* *1.9. Тема: Защита виртуальной инфраструктуры организации.* *1.10. Тема: Защита информации мобильных устройств и приложений.* *1.11.Тема: Критическая информационная инфраструктура организаций.* *1.12. Подготовка к защите лабораторных работ.* *1.13. Выполнение расчетно-графической работы.*

Текущий контроль:

Индикаторы достижения компетенции	Вид текущего контроля	Тема
ПК-1.1 Вырабатывает варианты реализации требований к программному обеспечению и анализирует возможности их реализации. ПК-1.2 Проектирует структуры данных, базы данных, программные интерфейсы, информационные системы по видам обеспечения. ПК-1.3 Разрабатывает и адаптирует компоненты, модули прикладного программного обеспечения	Защита лабораторных работ. Проверка выполнения заданий расчетно-графической работы. Проверка отчета по расчетно-графической работе. Проверка конспектов лекций. Собеседование.	*Тема: Международные стандарты информационного обмена. Понятие угрозы. Концепция информационной безопасности. Виды противников (или «нарушителей»).* *Тема: Основные положения теории информационной безопасности информационных систем.* *Тема: Виды возможных нарушений информационных систем. Особенности нарушений информационных систем в конкретных предметных областях.* *Тема: Критическая информационная инфраструктура организаций.*
ПК-5.1 Анализирует и формализует требования к информационным ресурсам, предлагает варианты реализации информационных ресурсов и осуществляет коммуникации с заинтересованными лицами ПК-5.2 Осуществляет админи-	Защита лабораторных работ. Проверка выполнения заданий расчетно-графической работы. Проверка отчета по расчетно-графической работе. Проверка конспектов лекций. Собеседование.	*Тема: Использование защищенных компьютерных систем. Организация комплексной защиты.* *Тема: Методы криптографии. Защита данных. Шифрование данных и программ. Понятие идеального шифра.*

стрирование и эксплуатацию аппаратно-программных средств в соответствии с требованиями по защите информации		*Тема: Понятие о вредоносных программах. Виды компьютерных вирусов.* *Тема: Методы защиты информации в вычислительных сетях. Обеспечение информационной безопасности в глобальной сети Интернет.* *Тема: Критическая информационная инфраструктура организаций.*

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

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

№ п/п	Виды учебных занятий	Образовательные технологии
1	Лекции	Классическая (традиционная, информационная) лекция. Интерактивная лекция (проблемная лекция). Индивидуальные и групповые консультации по дисциплине.
2	Практические занятия	Технология обучения на основе решения задач и выполнения упражнений.
3	Лабораторная работа	Технология выполнения лабораторных заданий индивидуально. Технология проблемного обучения на основе анализа результатов лабораторной работы: групповая дискуссия, представление студентом или группой студентов (бригадой) результатов лабораторной работы в форме отчета. Проектная технология.
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: экзамен)	Технология устного опроса с учетом предварительных результатов рейтинговой система контроля.

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 защиты лабораторной работы «Защита от несанкционированного использования программ, основанная на привязке программного обеспечения к аппаратным средствам конкретного компьютера и использовании электронного ключа».

1. Какие виды аппаратных ключей Вы знаете?
2. Каковы особенности механизма идентификации и аутентификации пользователей Вы знаете?
3. Какие аппаратные идентификаторы могут применяться в системе защиты?
4. Возможно ли в обеспечить идентификацию и аутентификацию пользователей до загрузки операционной системы (ОС)?
5. Что представляют собой биометрические системы идентификации?
6. Проанализируйте достоинства и недостатки биометрической системы идентификации.
7. Приведите примеры аппаратно-программных решения в области аутентификации и защиты информации.

Вопросы для защиты лабораторной работы «Изучение и использование различных методов криптографии для защиты данных. Ассиметричные криптоалоритмы».

1. Что такое открытый и закрытый ключи шифрования?
2. В чем особенности асимметричных криптосистем?
3. Что понимают под идеальным ключом шифрования?
4. Как формируются открытый и закрытый ключи шифрования?
5. Приведите примеры программных инструментов реализующих ассиметричные алгоритмы шифрования.
6. В чем отличие шифрования от тайнописи?

Вопросы для защиты лабораторной работы «Изучение и использование различных методов криптографии для защиты данных. Симметричные криптоалоритмы».

1. Что означает принцип "диффузии" в любом алгоритме шифрования.
2. Проведите сравнительную характеристику симметричных и асимметричных криптосистем.
3. Назовите отличительные особенности симметричных криптосистем.
4. Что означает принцип "конфузии"?
5. Приведите примеры программных инструментов реализующих симетричные алгоритмы шифрования.
6. Для чего используют аппаратные шифраторы?

Вопросы для защиты лабораторной работы «Организация комплексной защиты информационной инфраструктуры организации. Критическая информационная инфраструктура организаций . Защита от несанкционированного доступа к информационным ресурсам. (Часть1.)»

1. Перечислите основные пути повышения ИБ организации?
2. Что представляю собой межсетевые экраны?
3. Что понимают под терминов «Демилитаризованная зона» в информационной безопасности?
4. Что представляет собой средства защиты обеспечивающие невозможность несанкционированного доступа в вычислительную систему?
5. Как можно организовать разграничение доступа к устройствам вычислительной системе?

6. Как можно обеспечить невозможность несанкционированной печати файлов на принтере?
7. Какие группы правил проверки сетевого трафика обычно реализуют в персональных межсетевых экранах (ПМЭ)?
8. Назовите наиболее характерные объекты КИИ.

Вопросы для защиты лабораторной работы «Организация комплексной защиты информационной инфраструктуры организации. Критическая информационная инфраструктура организаций. Обнаружение вторжений в информационную инфраструктуру организации. (Часть2.)»

1. Для каких целей используются системы обнаружения вторжений?
2. Какие события считаются событиями тревоги?
3. Как администратор ИБ должен обрабатывать тревоги?
4. Где хранятся сведения о тревогах в вычислительной сети? Как хранятся записи журналов безопасности?
5. Что представляет собой пентестинг (испытание на проникновение)?
6. Назовите основные методы пентестинга?
7. Приведите примеры наиболее известных на текущий момент систем обнаружения вторжений.
8. Как реализуется взаимодействие с системой ГОССОПКА?

Вопросы для собеседования на практическом занятии «Нормативная и законодательная база РФ, обеспечивающая функционирование систем защиты информации».

1. Какие стандарты, необходимо использовать при разработке ПИБ организации?
2. Какие элементы должна содержать политика информационной безопасности (ПИБ) организации?
3. Перечислите основные шаги по разработке ПИБ организации.
4. Какие элементы должна содержать должностная инструкция специалиста по информационной безопасности организации?
5. Перечислите основные ФЗ России по обеспечению информационной безопаснсости.
6. Что понимают под конфиденциальностью информации?
7. Какие основные вопросы регламентирует Федерального закон РФ от 27 июля 2006 г. N 152-ФЗ «О персональных данных?

Вопросы для собеседования на практическом занятии «Изучение программных средств, обеспечивающих защиту от вредоносных программ».

1. Приведите примеры наиболее популярных антивирусных программ.
2. Какие технологии поиска вредоносных программ используют антивирусные программы?
3. Что представляет собой эвристический поиск вредоносных программ?
4. Перечислите основные типы вредоносных программ.
5. Что представляет собой поиск сигнатур вредоносных программ?
6. Перечислите способы внедрения и механизмы активации вредоносных программ.
7. Какие вредоносные последствия могут наблюдаться в результате внедрения (заражения) вредоносными программами?

Вопросы для собеседования на практическом занятии «Основы аудита информационной безопасности. Общая система оценки уязвимостей».

1. Что представляет собой и как работает общая система оценки уязвимостей (Common Vulnerability Scoring System – CVSS)?
2. Кто выполняет оценку и кто владеет CVSS?
3. Как необходимо использовать CVSS?

4. Перечислите метрические группы.
5. Перечислите и поясните базовые показатели.
6. Перечислите и поясните временные показатели.
7. Перечислите и поясните экологические показатели.
8. Что содержит описание каждой метрика в векторе?

Вопросы для собеседования на практическом занятии «Информационные системы персональных данных. Организация и ведение работ по обеспечению безопасности персональных данных при их обработке в информационных системах ПнД».

1. Что представляют собой ИСПнД? Приведите примеры ИСПнД.
2. Составить перечень основных нормативных правовых актов, регулирующих правовые отношения в области защиты персональных данных.
3. Дать определения следующих понятий: персональные данные, субъект и оператор персональных данных, обработка персональных данных, в том числе и автоматизированная, информационная система персональных данных, категории персональных данных.
4. Определить права субъектов персональных данных и обязанности оператора персональных данных.
5. Рассмотреть административную и уголовную ответственность за нарушения российского законодательства по обработке персональных данных.
6. Что представляет собой двухфакторная аутентификация?
7. Какие классы защищенности ИСПнД Вы знаете?
8. Что представляет собой «фишинг»?
9. Как используют методы социальной инженерии для хищения ПнД?
10. Сформулируйте кратко назначение единой системы идентифкации и аутентификации РФ (ЕСИА).

Вопросы для собеседования на практическом занятии « Основные принципы защищенного электронного документооборота. Электронная цифровая подпись».

1. Какие существуют виды электронной цифровой подписи (ЭЦП)?
2. Дайте понятие ЭЦП (согласно Федеральному закону от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи").
3. Придает ли усиленная квалифицированная ЭЦП документам юридическую силу без дополнительных условий? Ответ поясните.
4. Какую информацию содержит в себе ЭЦП?
5. Приведите примеры программных средств реализующих работу с ЭЦП?
6. Перечислите основные шаги в процессе применения ЭЦП.

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 8-м семестре.*

Оценочные средства промежуточной аттестации

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

1. Основные понятия и определения информационной безопасности.
2. Виды и источники угроз безопасности информации.

3. Классификация угроз информационной безопасности.
4. Методы и средства защиты информации.
5. Правовые меры обеспечения информационной безопасности.
6. Законодательные и нормативные акты Российской Федерации в области защиты информации.
7. Критерии оценки безопасности компьютерных систем.
8. Защита программного обеспечения, основанная на идентификации аппаратного и программного обеспечения.
9. Электронные ключи.
10. Организационно-административные методы защиты информационных систем.
11. Формирование политики информационной безопасности организации.
12. Основные принципы формирования пользовательских паролей.
13. Идентификация пользователей (назначение и способы реализации).
14. Аутентификация пользователей (назначение и способы реализации).
15. Авторизации пользователей (назначение и способы реализации).
16. Криптографические методы защиты информации.
17. Симметричные криптосистемы.
18. Поточные шифры.
19. Свойства синхронных и асинхронных поточных шифров.
20. Шифры подстановки и перестановки.
21. Блочные шифры.
22. Шифр Файстеля.
23. Асимметричные криптосистемы.
24. Алгоритм шифрования RSA.
25. Реализация алгоритмов шифрования.
26. Электронная цифровая подпись.
27. Защита информации в компьютерных сетях.
28. Объекты защиты информации в сети.
29. Уровни сетевых атак согласно эталонной модели взаимодействия открытых систем OSI.
30. Потенциальные угрозы безопасности в Internet.
31. Методы защиты информации в сети Internet.
32. Использование межсетевых экранов для обеспечения информационной безопасности в Internet. Классификация межсетевых экранов.
33. Схемы подключения межсетевых экранов.
34. Частные виртуальные сети (VPN). Классификация VPN.
35. Защита информации на уровне межсетевого протокола Internet Protocol (IP). Протокол IPSecurity.
36. Методы защиты от вредоносных программ («червей», «троянских программ» и т.д.).
37. Анализ рынка антивирусных программ.
38. Комплексная защита информационных систем.
39. Политика информационной безопасности организации.
40. Защита персональных данных.

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

- реализация синтеза ключей шифрования;
- определение цикловых ключей шифрования;

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

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

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

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; персональными компьютерами с подключением к сети "Интернет".

Для проведения занятий лабораторного типа

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

- специализированной мебелью; доской аудиторной; персональными компьютерами с подключением к сети "Интернет".

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

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

Программное обеспечение

При проведении лабораторных работ предусматривается использование программного обеспечения: Виртульный программный лабораторный стенд «Secret Net Studio» от «Код безопасности», Delphy (в составе Embarcadero RAD Studio), антивирусные программы.

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 Шаньгин В.Ф. Информационная безопасность [электронный ресурс]: учебное пособие/ Шаньгин В.Ф. - М. Изд. «ДМК Пресс», 2014. – 702с. Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=50578

2 Андрианов В.В., Зефиров С.Л. и др. Обеспечение информационной безопасности бизнеса [электронный ресурс]. М.: Альпина Паблишерз, 2011 – 373 с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=235577&sr=1

Дополнительная литература.

1 Аверченков В.И. Аудит информационной безопасности [электронный ресурс]: учебное пособие/ В.И. Аверченков. М. :Флинта, 2011 – 269с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=93245&sr=1

2 Беломойцев Д.Е., Волосатова Т.М., Радионов С.В. Основные методы криптографической обработки данных [электронный ресурс]: учебное пособие / Беломойцев Д.Е. – М. Изд. МГТУ им. Н.Э. Баумана (Московский государственный технический университет имени Н.Э. Баумана), 2014. – 76с. Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=58438

3 Бирюков А.А. Информационная безопасность: защита и нападение [электронный ресурс]: учебник / Бирюков А.А. – М. Изд. «ДМК Пресс», 2012. – 474с. Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=39990

4 Information Security / Информационная безопасность. Журнал [электронный ресурс]: http://www.itsec.ru/main.php

Список авторских методических разработок.

1 Окунев Б.В. Методические указания по выполнению расчетно-графической работы по дисциплине "Информационная безопасность" : (для студентов направления 09.03.03 "Прикладная информатика") / Б.В. Окунев ; 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 .— 19 с. : ил., табл. ; 1 файл: 218 Кб .— Загл. с титул. экрана .— Системные требования: Acrobat Reader .— Электрон. копия представлена на сайте Библиотеки вуза .— б.ц. — <URL:http://lib.sbmpei.ru/file/upload/L_40.pdf>

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