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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: 09.04.03 «Прикладная информатика»

Магистерская программа «Информационные системы и технологии в управлении бизнес–процессами»

Уровень высшего образования: магистратура

Нормативный срок обучения: 2 года

Форма обучения: очная

Год набора: 2023

Смоленск

Программа составлена с учетом ФГОС ВО – магистратура по направлению подготовки 09.04.03 Прикладная информатика, утвержденного приказом Минобрнауки России от «19» сентября 2017 г. № 916, с изменениями, внесенными приказом Минобрнауки России от «26» ноября 2020 г. № 1456.

Программу составил:

канд. техн. наук, доц. _____ Б.В. Окунев
подпись ФИО

«20» января 2023 г.

Программа обсуждена и одобрена на заседании кафедры информационных технологий в экономике и управлении
«07» февраля 2023 г., протокол № 6

Заведующий кафедрой информационных технологий в экономике и управлении:

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

«08» февраля 2023 г.

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Ответственный в филиале по работе
с ЛОВЗ и инвалидами

_____ Е.В. Зуева
подпись ФИО

«08» февраля 2023 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является подготовка обучающихся к решению задач профессиональной деятельности научно-исследовательского и организационно-управленческого типов в области информационных и коммуникационных технологий по направлению подготовки 09.04.03 Прикладная информатика (магистерская программа: Информационные системы и технологии в управлении бизнес–процессами) 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 с современными угрозами в ИТ-сфере;
- ознакомить с нормативно-правовыми документами в сфере информационной безопасности;
- сформировать умения сбора и анализа информации для формализации требований заказчика по обеспечению защиты информационных ресурсов;
- сформировать умения оценки рисков от реализации угроз информационной безопасности;
- выработать способности безопасного коммуницирования с заказчиком;
- 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.
- развить навыки определения угроз информационной безопасности в организации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина Методы и средства защиты компьютерной информации относится *к части, формируемой участниками образовательных отношений.*

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

Б1.В.01 Управление информационными ресурсами
Б1.В.02 Управление бизнес-процессами и реинжиниринг информационных процессов
Б1.В.ДВ.01.01 Управление качеством информационных систем
Б1.В.ДВ.01.02 Современные технологии баз и банков данных

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

Б1.В.ДВ.02.01 Предпринимательство в информационной сфере
Б1.В.ДВ.02.02 Маркетинговый анализ рынка информационных технологий
Б2.В.02(Н) Научно-исследовательская работа
Б2.В.03(П) Технологическая (проектно-технологическая) практика
Б2.В.04(Пд) Преддипломная практика
Б3.01 Подготовка к защите и защита выпускной квалификационной работы

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины направлено на формирование элементов следующих компетенций в соответствии с 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-1. Способен проводить научно-исследовательские и опытно-конструкторские разработки при исследовании самостоятельных тем	ПК-1.1 Организует сбор и изучение научно-технической информации по теме исследований и разработок	Знает: основные современные научные принципы и методы научных исследований в области информационной безопасности (ИБ). Умеет: обосновывать выбор метода исследований в сфере защиты информации Владеет: навыками эффективного сбора научно-технической информации в сфере ИБ.
	ПК-1.2 Проводит анализ научных данных, результатов экспериментов и наблюдений	Знает: основные методы анализа научных данных в сфере ИБ. Умеет: проводить анализ результатов экспериментов в сфере ИБ. Владеет: навыками обработки и анализа результатов экспериментов в сфере ИБ.
	ПК-1.3 Осуществляет теоретическое обобщение научных данных, результатов экспериментов и наблюдений	Знает: основные этапы проведения анализа результатов экспериментов в сфере ИБ. Умеет: обобщать результаты наблюдений и делать правильные научные выводы в области ИБ. Владеет: навыками применения современных научных принципов и методов в области информационной безопасности.
ПК-2. Способен управлять ресурсами информационных технологий	ПК-2.3 Формирует цели, требования и приоритеты управления информационной безопасностью ресурсов ИТ, организует процесс управления информационной безопасностью ресурсов ИТ	Знает: основные методы управления IT-ресурсами организаций. Умеет: обосновывать выбор методов управления IT-ресурсами организаций Владеет: навыками применения методов управления IT-ресурсами организаций.
ПК-5. Способен управлять программно-техническими, технологическими и человеческими ресурсами	ПК-5.2 Выявляет и отслеживает риски в процессе разработки программного обеспечения	Знает: основные методы выявления рисков в процессе разработки ПО Умеет: проводить анализ причин возникновения различных рисков в процессе разработки ПО Владеет: навыками выявления рисков в процессе разработки ПО.
	ПК-5.3 Проводит структурную декомпозицию работ, определяет критерии оценки сложности, трудоемкости и сроков выполнения работ	Знает: основные критерии оценки сложности и трудоемкости работ по созданию ПО. Умеет: оценить сроки выполнения работ при создании ПО в сфере ИБ. Владеет: навыками проведения декомпозиции работ и оценке их трудоемкости в процессе создания ПО в сфере ИБ.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Структура дисциплины:

№	Индекс	Наименование	Семестр 3											Семестр 4											Итого за курс												
			Контроль	Академических часов								з.е.	Недель	Контроль	Академических часов								з.е.	Недель	Контроль	Академических часов								з.е.	Недель	Каф.	Семестры
				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			
3	Б1.В.04	Методы и средства защиты компьютерной информации	Эк	252	66	34	32			150	36	7													Эк	252	66	34	32			150	36	7		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: 1.1. Основные положения теории информационной безопасности. 1.2. Основные нормативные руководящие документы, законы РФ и т.п. касающиеся государственной тайны и защиты информации. 1.3. Защита программного обеспечения, основанная на идентификации пользователя и ПК. 1.4. Защита программного обеспечения, основанная на идентификации исполняемого модуля. 1.5. Основы криптографических методов защиты информации. 1.6. Симметричные криптосистемы. 1.7. Ассиметричные криптосистемы. 1.8. Использование криптографических методов защиты информации. 1.9. Виды вредоносных программ (компьютерных вирусов). 1.10. Методы борьбы с вредоносными программами. 1.11. Организация защиты персональных данных в информационных системах персональных данных. 1.12. Основные принципы защищенного электронного документооборота. Электронная цифровая подпись. 1.13. Политика информационной безопасности организации. 1.14. Организация комплексной защиты автоматизированных ИС. 1.15. Применение сертифицированных средств комплексной защиты информации в организациях на примерах конкретных решений. 1.16. Таксономия нарушений информационной безопасности. Аттестация объектов информатизации по требованиям безопасности. 1.17. Оценка надежности и эффективности защитных механизмов.
2	Лабораторные работы 8 шт. по 4 часа: 2.1. Организация комплексной защиты информационной инфраструктуры организации. Знакомство с основными возможностями и настройка лабораторного стенда по ИБ. 2.2. Организация комплексной защиты информационной инфраструктуры организации. Дискреционное управление доступом к информационным ресурсам. 2.3. Организация комплексной защиты информационной инфраструктуры организации. Полномочное управление доступом к информационным ресурсам. 2.4. Организация комплексной защиты информационной инфраструктуры организации. Межсетевой экран. 2.5. Организация комплексной защиты информационной инфраструктуры организации. Защита от вирусов и вредоносного ПО. 2.6. Организация комплексной защиты информационной инфраструктуры организации. Обнаружение вторжений в информационную инфраструктуру организации. 2.7. Организация комплексной защиты информационной инфраструктуры организации. Исследование и оценка эффективности защитных механизмов с помощью тестирования на проникновение (пентестинг). 2.8. Применение электронной цифровой подписи.
3	Самостоятельная работа студентов: 3.1. Тема: Угрозы безопасности персональных данных, уязвимости информационных систем ПнД. 3.2. Тема: Базовая модель угроз безопасности ПнД.

	3.3. Тема: Организация физическим лицом защиты своих персональных данных. 3.4. Тема: Виды, источники и классификация угроз информационной безопасности. 3.5. Тема: Актуальный банк данных угроз информационной безопасности. 3.6. Тема: Системы обнаружения вторжений. 3.7. Тема: Аудит информационной безопасности. 3.8. Тема: Частные виртуальные сети. 3.9. Тема: Защита виртуальной инфраструктуры организации. 3.10. Тема: Защита информации мобильных устройств и приложений 3.11. Подготовка к защите лабораторных работ.

Текущий контроль:

Индикаторы достижения компетенции	**Вид текущего контроля**	**Тема**
ПК-1.1 Организует сбор и изучение научно-технической информации по теме исследований и разработок. ПК-1.2 Проводит анализ научных данных, результатов экспериментов и наблюдений. ПК-1.3 Осуществляет теоретическое обобщение научных данных, результатов экспериментов и наблюдений.	Защита лабораторных работ. Проверка конспектов лекций.	*Тема: Основные положения теории информационной безопасности.* *Тема: Основные нормативные руководящие документы, законы РФ и т.п. касающиеся государственной тайны и защиты информации.* *Тема: Аудит информационной безопасности.* *Тема: Угрозы безопасности персональных данных, уязвимости информационных систем ПнД.*
ПК-2.3 Формирует цели, требования и приоритеты управления информационной безопасностью ресурсов ИТ, организует процесс управления информационной безопасностью ресурсов ИТ	Защита лабораторных работ. Проверка конспектов лекций. Собеседование.	*Тема: Политика информационной безопасности организации.* *Тема: Организация защиты персональных данных в информационных системах персональных данных.* *Тема: Основы криптографических методов защиты информации.* *Тема: Виды вредоносных программ (компьютерных вирусов).* *Тема: Методы борьбы к вредоносными программами.*
ПК-5.2 Выявляет и отслеживает риски в процессе разработки программного обеспечения. ПК-5.3 Проводит структурную декомпозицию работ, определяет критерии оценки сложности, трудоемкости и сроков выполнения работ	Защита лабораторных работ. Проверка конспектов лекций.	*Тема: Организация комплексной защиты автоматизированных ИС.* *Тема: Основные принципы защищенного электронного документооборота. Электронная цифровая подпись.* *Тема: Базовая модель угроз безопасности ПнД.*

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	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.
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 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 «Организация комплексной защиты информационной инфраструктуры организации. Знакомство с основными возможностями и настройка лабораторного стенда по ИБ»

1. Перечислите основные возможности лабораторного стенда по организации комплексной защиты ИБ.
2. Назовите способы развертывания компонентов лабораторного стенда по ИБ.
3. Какие механизмы защиты реализованы в предлагаемом лабораторном стенед?
4. Каким образом производится настройка компонентов защиты?
5. Как производится настройка контроля аудита в системе защиты лабораторного стенда?
6. Какие элементы должна содержать политика информационной безопасности (ПИБ) организации?

Вопросы для защиты лабораторной работы «Организация комплексной защиты информационной инфраструктуры организации. Дискреционное управление доступом к информационным ресурсам»

1. Что представляет собой дискреционное (избирательное) управление доступом к информационным ресурсам организации?
2. Как назначаются привилегии управления доступом к файловым ресурсам при дискреционном управлении доступом?
3. В чем достоинства и недостатки дискреционного управления доступом к информационным ресурсам организации?
4. Как проводятся настройки аудита операций с ресурсами при дискреционном управлении доступом к информационным ресурсам организации?
5. Что представляет собой матрица доступа к информационным ресурсам при дискреционном управлении доступом?
6. Перечислите множество обычных типов доступа субъектов к объектам ресурсам при дискреционном управлении доступом.

Вопросы для защиты лабораторной работы «Организация комплексной защиты информационной инфраструктуры организации. Полномочное управление доступом к информационным ресурсам».

1. Что представляет собой полномочное (мандатное) управление доступом к информационным ресурсам организации?
2. Как обеспечивается разграничение доступа пользователей к конфиденциальным ресурсам
3. Опишите работу механизма полномочного разграничения доступа к информационным ресурсам организации.
4. В чем достоинства и недостатки полномочного управления доступом к информационным ресурсам организации?
5. Как проводятся настройки аудита операций с ресурсами при полномочном управлении доступом к информационным ресурсам организации?
6. Каким образом формируется состав используемых категорий конфиденциальности и перечень ресурсов при полномочном управлении доступом?

Вопросы для защиты лабораторной работы «Организация комплексной защиты информационной инфраструктуры организации. Межсетевой экран».

1. Каково назначение межсетевых экранов (МЭ)?
2. Какие схемы включения межсетевых экранов Вы знаете?
3. Что понимают под термином «Демилитаризованная зона» в информационной безопасности?
4. Как настраиваются правила для механизма работы МЭ?
5. Какие группы правил проверки сетевого трафика обычно реализуют в персональных межсетевых экранах (ПМЭ)?
6. Приведите классификацию МЭ по различным признакам.

Вопросы для защиты лабораторной работы «Организация комплексной защиты информационной инфраструктуры организации. Защита от вирусов и вредоносного ПО»

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 защиты лабораторной работы «Организация комплексной защиты информационной инфраструктуры организации. Обнаружение вторжений в информационную инфраструктуру организации»

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. Приведите примеры наиболее известных на текущий момент систем обнаружения вторжений.

Вопросы для защиты лабораторной работы «Организация комплексной защиты информационной инфраструктуры организации. Исследование и оценка эффективности защитных механизмов с помощью тестирования на проникновение (пентестинг)».

1. Что представляет собой пентестинг (испытание на проникновение)?
2. Назовите основные методы пентестинга?
3. Как проводят оценку защитных механизмов?
4. Какие параметры используют для оценки качества защитных механизмов?
5. Назовите современные (наиболее популярные) инструменты для проведения пентестинга.

Вопросы для защиты лабораторной работы «Применение электронной цифровой подписи»

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 3-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. Защита программного обеспечения, основанная на идентификации аппаратного и программного обеспечения.
8. Электронные ключи.
9. Организационно-административные методы защиты информационных систем.
10. Формирование политики безопасности организации.
11. Основные принципы формирования пользовательских паролей.
12. Идентификация пользователей (назначение и способы реализации).
13. Аутентификация пользователей (назначение и способы реализации).
14. Авторизации пользователей (назначение и способы реализации).
15. Криптографические методы защиты информации.
16. Симметричные криптосистемы.
17. Свойства синхронных и асинхронных поточных шифров.
18. Основные особенности стандарта шифрования DES.
19. Стандарт шифрования ГОСТ 28147-89.
20. Асимметричные криптосистемы.
21. Алгоритм шифрования RSA.
22. Сравнительная характеристика симметричных и асимметричных алгоритмов шифрования.
23. Электронная цифровая подпись.
24. Методы защиты информации в сети Internet.
25. Использование межсетевых экранов для обеспечения информационной безопасности в Internet.
26. Классификация межсетевых экранов. Схемы подключения межсетевых экранов.
27. Частные виртуальные сети (VPN). Классификация VPN.
28. Количественный подход к информационной безопасности. Оценка защищенности механизмов защиты.
29. Методы защиты от вредоносных программ («червей», «троянских программ» и т.д.).
30. Анализ рынка антивирусных программ.
31. Комплексная защита информационных систем.
32. Организация защиты программного обеспечения от исследования.

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)»/	Выставляется обучающемуся, обнаружившему всестороннее, систематическое и глубокое знание материалов изученной дисциплины, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с до-

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
«зачтено»	полнительной 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 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», 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 Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации [электронный ресурс] : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=276557

2 Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях [электронный ресурс] : учебное пособие / М.А. Иванов, И.В. Чугунков ; Министерство образования и науки Российской Федерации, Национальный исследовательский ядерный университет «МИФИ» ; под ред. М.А. Иванов. - М. : МИФИ, 2012. - 400 с. Режим доступа : http://biblioclub.ru/index.php?page=book&id=231673

Дополнительная литература.

1 Разработка моделей криптографической защиты информации [электронный ресурс] : монография / В.Г. Шубович, В.В. Капитанчук, Н.С. Знаенко, Ю.И. Титаренко ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Ульяновский государственный педагогический университет имени И.Н. Ульянова». - Ульяновск : УлГПУ, 2013. - 128 с. Режим доступа : http://biblioclub.ru/index.php?page=book&id=278070

2 Разрушающие программные воздействия / . - М. : МИФИ, 2011. - 328 с. Режим доступа : http://biblioclub.ru/index.php?page=book&id=231881

3 Основы применения системы защиты Secret Net Studio. Учебно-методическое пособие. - М.: Код безопасности, 2017. - 207 с.

4 Лаборатория Касперского [электронный ресурс]: http://www.kaspersky.ru

5 Сервисы сетевой безопасности от «Код безопасности» [электронный ресурс]: https://www.securitycode.ru

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Номера страниц				Всего страниц в документе	Наименование и № документа, вводящего изменения	Подпись, Ф.И.О. внесшего изменения в данный экземпляр	Дата внесения изменения в данный экземпляр	Дата введения изменения
	измененных	замененных	новых	аннулированных					
1	2	3	4	5	6	7	8	9	10