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

УТВЕРЖДАЮ
Зам. директора
по учебно-методической работе
филиала ФГБОУ ВО
«НИУ «МЭИ» в г. Смоленске
_____ В.В. Рожков
«28» 08 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИ-ЦИ-
ОННОЙ БЕЗОПАСНОСТИ
(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: 10.04.01 Информационная безопасность

Магистерская программа: «Безопасность автоматизированных систем»

Уровень высшего образования: магистратура

Нормативный срок обучения: 2 года

Форма обучения: очная

Год набора: 2021

Смоленск – 2021 г.

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

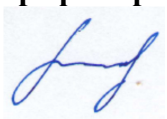
Программу составил:
к.т.н., доцент кафедры «Вычислительная техника»

Я.А. Федулов

«27» июня 2021 г.

Программа обсуждена и одобрена на заседании кафедры «Вычислительная техника»
«30» июня 2021 г., протокол № 11

Заведующий кафедрой вычислительной техники
д.т.н., профессор



А.С. Федулов

«02» июля 2021 г.

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Ответственный в филиале по работе
с ЛОВЗ и инвалидами

Е.В. Зуева

«02» июля 2021 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Технологии обеспечения информационной безопасности» является формирование комплекса знаний, навыков и компетенций в области информационной безопасности и применения на практике методов и средств защиты информации на основе современных интеллектуальных технологий, средств и языков программирования.

Задачами дисциплины являются: изучение основных понятий и определений, классификаций современных тенденций и угроз информационной безопасности; получение знаний об о нормативных правовых документах по защите информации; получение навыков разработки оригинальных алгоритмов и программных средств, в том числе с использованием современных интеллектуальных технологий; формирование у студентов устойчивого понимания роли и значения информационной безопасности личности, общества, государства и информационной инфраструктуры общества и государства; получение навыков разработки компонентов программно-аппаратных комплексов обработки информации и автоматизированного проектирования; выработка практических навыков применения современных методов и средств защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Технологии обеспечения информационной безопасности» относится *к части, формируемой участниками образовательных отношений* профессионального цикла Б1.В.03 основной образовательной программы подготовки магистров по направлению «10.04.01 «Информационная безопасность».

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

Б1.О.03 Управление информационной безопасностью (УК-1; ОПК-1; ОПК-3).

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

Б1.О.07 Защищенные информационные системы (ОПК-1; ОПК-2).

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 (*специальности*):

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы достижения компетенций	Результаты обучения
ОПК-1. *Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.*	***ОПК-1.1.*** *Обосновывает требования к системе обеспечения информационной безопасности.* ***ОПК-1.2.*** *Разрабатывает проект технического задания на создание системы обеспечения информационной безопасности.*	***Знает:*** *принципы и средства организации защиты информационных систем; основные угрозы информационной безопасности систем; методы и способы обеспечения защиты информации программными и программно-аппаратными средствами.* ***Умеет:*** *разрабатывать требования к компонентам систем информационной безопасности, оценивать технические решения по защите компьютерных ресурсов от несанкционированного доступа, на уровне серверов и рабочих станций в закрытых и открытых контурах вычислительных сетей.* ***Владеет:*** *методологией разработки требований к защищенным информационным системам; навыками и методами формирования политик информационной безопасности; навыками проектирования и создания защищенных информационных систем.*
ОПК-2. *Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.*	***ОПК-2.1.*** *Выбирает методологию и технологию проектирования систем (подсистем либо компонентов системы) обеспечения информационной безопасности.* ***ОПК-2.2.*** *Разрабатывает технический проект системы (подсистемы либо компонента систе-*	***Знает:*** *угрозы и уязвимости проводных и беспроводных сетей; требования к проектированию защищенных информационных сетей; требования к обеспечению информации в «облачных» технологиях.* ***Умеет****:* *разрабатывать компоненты, обеспечивающие защиту информа-*

Компетенция	Индикаторы достижения компетенций	Результаты обучения
	мы) обеспечения информационной безопасности.	*ции; проектировать на их основе системы защиты информации, тестировать уровень защиты информации для различных типов угроз и проникновений.* ***Владеет**:* *методологией проектирования подсистем защиты информации, навыками разработки систем защиты информации на основе отдельных подсистем и системы в целом для локального и глобального уровней.*

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Индекс	Наименование	Семестр 2										Итого за курс									
		Кон-троль	Академических часов								з.е.	Кон-троль	Академических часов								з.е.
			Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Кон-троль			Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Кон-троль	Всего
Б1.О.05	Технологии обеспечения информационной безопасности	Экз РГР	**144**	68	34	34			40	36	4	Экз РГР	**144**	68	34	34			40	36	4

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. Основы информационной безопасности (ИБ).* Определение целей и принципов защиты информации; установление, факторов, влияющих на защиту информации; основные опасности и угрозы в области информационной безопасности. *1.2. Классификация методов и средств защиты информации.* Глубина классификации и реквизит. Классификации видов, методов и средств защиты информации. Организационная защита информации. Инженерно-техническая защита информации. Криптографическая защита информации. Представление информации в цифровом виде. *1.3. Задачи информационной безопасности.* Задача обеспечения конфиденциальности. Задача обеспечения доступа. Задача обеспечения аутентификации. Обеспечение идентификации. Задача обеспечения целостности. *1.4. Угрозы информационной безопасности.* Классификация угроз информационной безопасности. Угрозы несанкционированного доступа к данным. Угрозы нарушения целостности данных. Угрозы нарушения конфиденциальности данных. *1.5. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере.* Основы законодательства в области обеспечения информационной безопасности. Правовое обеспечение информационной безопасности. Российское законодательство в области информационной безопасности. Закон «Об информации, информатизации и защите информации». Защита персональных данных. Другие законы и нормативные акты. *1.6. Понятие и виды защищаемой информации.* Путь конфиденциального документа от создания до уничтожения: решение, разработка проекта, подготовка содержания, реквизитов, передача, получение, исполнение и архивация. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Защита конфиденциальной информации при ее передаче по сети. Система защищенного электронного документооборота. *1.7. Защита информации. Общая характеристика способов и средств защиты информации.* Способы и средства защиты информации от несанкционированного доступа. Способы и средства защиты информации от вредоносного кода. Способы и средства защиты информации от межсетевого воздействия. Способы и средства криптографической защиты информации. *1.8. Криптографические методы защиты информации.* Основные понятия и термины криптографии. Краткая история развития шифров. Примеры. Основные проблемы криптографии. Парадоксы. Оценка секретных систем. Криптостойкость. Методы криптоанализа и взлома. *1.9. Криптографические методы защиты информации. Одностороннее шифрование.* Виды алгоритмов хэширования. Алгоритмы выработки имитовставки. Гаммирование. Хэш- функции. Семейство алгоритмов SHA. *1.10. Криптографические методы защиты информации. Симметричной шифрование.* Виды алгоритмов хэширования. Алгоритмы выработки имитовставки. Гаммирование. Хэш- функции. Алгоритм SHA. Симметричные шифры. Криптография с открытым ключом. Блочные и потоковые шифры. Алгоритмы DES, AES.

	1.11. Криптографические методы защиты информации. Асимметричной шифрование. Ассиметричное шифрование, преимущества и недостатки. Понятие открытого и закрытого ключа. Алгоритм Диффи – Хеллмана. Схема алгоритма RSA. *1.12. Электронная цифровая подпись и цифровые сертификаты.* Электронная цифровая подпись. Понятие о цифровой подписи. Подпись RSA. Подпись ElGamal. Подпись DSA.ЭЦП ГОСТ Р 34.10-94 и ГОСТ Р 34.10-01. Инфраструктура открытых ключей. Сертификаты открытых ключей. *1.13. Обеспечение высокой доступности, туннелированные и управление.* Методы и средства обеспечения высокой доступности. Проактивное управление, задание реакций, резервное копирование. Синхронное и асинхронное тиражирование. Туннелирование данных. Мониторинг и контроль. *1.14. Практические аспекты криптографии.* Способы взлома и кражи данных в сетях. Защита протоколаWiFi. Протокол HTTPs. Виртуальные персональные сетевые каналы VPS. Схема работы протокола TOR. Сетевой протокол прикладного уровня, позволяющий производить удалённое управление SSH. *1.15. Методы организации безопасного доступа.* Схемы идентификации и аутентификации. Одно- и многофакторная аутентификация. Система разграничения доступа к информации в компьютерной системе. Концепция построения систем разграничения доступа. Средства и методы ограничения доступа к файлам. *1.16. Программно-аппаратные средства защиты информации.* Аппаратные и программно-аппаратные средства криптозащиты данных. Использование дополнительных плат расширения. Методы «водяных знаков» и методы «отпечатков пальцев». Защита программ от несанкционированного копирования. *1.17. Классификация вирусов. Применение антивирусных программ.* Классификация вирусных программ. Основные признаки заражения от вредоносных программ. Методы заражения. История антивирусных программ, сведения о надежности и механизмах работы современных антивирусных программ. Основные моменты использования современных антивирусных программ.
2	Лабораторные работы 9 шт. по 4 (2) часа: *2.1. Перехват и анализ сетевых пакетов.* Изучить возможности библиотеки WinPcap, Изучить возможности библиотеки SharpPcap; осуществить перехват и анализ сетевых пакетов на сетевом транспортном и прикладном уровнях модели OSI. *2.2. Современные симметричные криптосистемы.* Изучение принципов работы симметричных криптосистем, многие из которых являются национальными или ведомственными стандартами; изучение реализаций симметричной криптографии в среде .NET Framework; программная реализация существующих симметричных криптоалгоритмов. *2.3. Современные асимметричные криптосистемы.* Изучение принципов работы асимметричных криптосистем; изучение реализаций асимметричной криптографии в среде .NET Framework; реализация существующих асимметричных криптоалгоритмов. 2.4. *Хэширование и электронная цифровая подпись.* Изучение методов формирования дайджеста сообщения (хэш-функции) и электронной цифровой подписи (ЭЦП); изучение реализаций хэш-функций и ЭЦП в среде .NET Framework; реализация существующих хэш-функций и алгоритмов ЭЦП. *2.5. Работа с системными журналами в операционной системе.* Изучение методов работы с системными журналами. Отслеживание событий записи в системные журналы. Перехват системных событий. Анализ записей системных журналов. *2.6. Работа с системными журналами в операционной системе. Файловая система.* Отслеживание событий изменения файловой системы (создание, удаление, переименование и

	изменение выбранных файлов и папок). Отслеживание событий изменения аппаратной конфигурации компьютера. *2.7. Удаленный доступ и управление операционной системой.* Удаленный доступ к ресурсам операционной системы с использованием технологии WMI. Знакомство с утилитой командной строки wmic. Работа с протоколом удаленного доступа SSH. *2.8. Управление политиками безопасности.* Исследование методов контроля доступа к ресурсам операционной системы. Обеспечение безопасности доступа кода (утверждение и отклонение полномочий). Управление политиками безопасности. *2.9. Практическая реализация распределения ключей.* Безопасное распределение ключей. Алгоритм Диффи-Хеллмана.
3	Практические занятия не предусмотрены в курсе дисциплины.
4	Курсовая работа не предусмотрена в структуре дисциплины.
5	Расчетно-графическая работа студентов выдается согласно индивидуально выбранной теме и включает следующие этапы: постановка задачи разработки защищенного алгоритма; обзор, сравнительный анализ и подбор подходящих стандартов информационной безопасности; формирование требований к применению алгоритма; формирование и реализация функциональных требований; этапы построения и реализации защищенного алгоритма на практике. Примеры индивидуальных тем на разработку защищенного алгоритма: 1) Разработка криптосистемы Ривеста-Шамира-Адлемана.. 2) Криптосистема, основанная на проблеме Диффи-Хеллмана.. 3) Разработка криптосистемы, основанной на эллиптических кривых. 4) Управление ключами, основанное на системах с открытым ключом. 5) Реализация системы потокового шифрования.
6	Самостоятельная работа студентов: 6.1. 2 контрольных опроса после 10-й и 17-й лекций; 6.2. Закрепление материала по тематике лекционных занятий: закрепление изучения материалов лекций 1.1-1.17 – основы разработки систем на языках высокого уровня; классификация методов и средств защиты информации; проектирование защищенного программного обеспечения; оценка качества разработанных защищенных программных средств системы; обеспечение уровней безопасности. 6.3. Подготовка к экзамену по дисциплине (оценочные материалы приведены в разделе 6 настоящей РПД).

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

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

№ п/п	Виды учебных занятий	Образовательные технологии
1	Лекции	Классическая (традиционная, информационная) лекция. Интерактивная лекция (лекция-визуализация). Индивидуальные и групповые консультации по дисциплине.
2	Лабораторная работа	Технология выполнения лабораторных заданий индивидуально. Технология выполнения лабораторных заданий в малой группе (в бригаде). Технология проблемного обучения на основе анализа результатов лабораторной работы: индивидуальный опрос, собеседование в малой группе (бригаде), обсуждение результатов командной работы, групповая дискуссия, метод «круглого стола», представление студентом или группой студентов (бригадой) результатов лабораторной работы в форме отчета и мультимедийной презентации. 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: зачет или экзамен)	Технология письменного контроля, в том числе тестирование. Рейтинговая 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 успеваемости:

Примеры вопросов к контрольному опросу после 10-й лекции:

1. Определение информационной безопасности.
2. Критические данные.
3. Признаки компьютерных преступлений в интернет технологиях.
4. Основные технологии и методы компьютерных преступлений.
5. Уровня защиты компьютерных (интернет технологий) и информационных ресурсов.
6. Признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности.
7. Концепция обеспечения безопасности информационных систем.
8. Избирательная политика управления доступом.

9. Организационные меры безопасности информационных систем.
10. Матрица доступа в АСОИ.
11. Полномочное управление доступом.
12. Избирательное управление доступом.
13. Оценочные стандарты и технические спецификации.
14. Угрозы безопасности данных
15. Источники нарушений безопасности
16. Аутентификация
17. Авторизация пользователей
18. Методы парольной аутентификации. Недостатки методов аутентификации с запоминаемым паролем.
19. Аутентификация с помощью биометрических характеристик.
20. Принципы работы биометрических систем.
21. Реализация биометрических систем.
22. Поведенческие биометрические характеристики.
23. Атаки на биометрические системы.

Примеры вопросов к контрольному опросу после 17-й лекции:

1. Основные понятия и термины криптографии. Краткая история развития шифров. Криптостойкость. Методы криптоанализа и взлома.
2. Криптографические методы защиты информации. Одностороннее шифрование.
3. Криптографические методы защиты информации. Симметричной шифрование.
4. Криптографические методы защиты информации. Асимметричной шифрование.
5. Электронная цифровая подпись и цифровые сертификаты.
6. Обеспечение высокой доступности, туннелированные и управление.
7. Практические аспекты криптографии.
8. Методы организации безопасного доступа.
9. Программно-аппаратные средства защиты информации.
10. Классификация вирусов. Применение антивирусных программ.

Примеры алгоритма самостоятельной работы по закреплению материала по тематике лекционных занятий:

В ходе изучения дисциплины «Технологии обеспечения информационной безопасности» студенты могут посещать аудиторные занятия (лекции, лабораторные занятия, консультации). Особенность изучения дисциплины состоит в выполнении комплекса лабораторных работ, главной задачей которого является получение навыков самостоятельной работы на компьютерах с использованием современных компьютерных программ, предназначенных для решения определенного круга профессиональных задач.

Важное место в овладении тем данной дисциплины отводится самостоятельной работе, при этом во время аудиторных занятий могут быть рассмотрены и проработаны наиболее важные и трудные вопросы по той или иной теме дисциплины, а более легкие вопросы могут быть изучены студентами самостоятельно.

Методика закрепления материалов лекционных занятий 1.1-1.17:

Закрепление знаний в области данной дисциплины, приобретение практических навыков проектирования программных автоматизированных систем с использованием структурного и объектно-ориентированного подходов осуществляется путем разработки программных средств по заданной предметной области.

Оценочные средства для промежуточной аттестации:

Примеры вопросов к экзамену по дисциплине:

1. Определение целей и принципов защиты информации; установление, факторов, влияющих на защиту информации; основные опасности и угрозы в области информационной безопасности.
2. Классификация методов и средств защиты информации. Глубина классификации и реквизит. Классификации видов, методов и средств защиты информации.
3. Задача обеспечения конфиденциальности. Задача обеспечения доступа. Задача обеспечения аутентификации. Обеспечение идентификации. Задача обеспечения целостности.
4. Классификация угроз информационной безопасности. Угрозы несанкционированного доступа к данным. Угрозы нарушения целостности данных. Угрозы нарушения конфиденциальности данных.
5. Защита информации. Основные понятия. Угрозы и меры защиты.
6. Виды атак. Сетевые атаки.
7. Виды политик информационной безопасности
8. Математические модели информационной безопасности. Модель Бела-Лападула и Биба
9. Математические модели информационной безопасности. Мандатная модель защиты от угроз ОВО
10. Математические модели информационной безопасности. Модель Харрисона-Руззо-Ульмана
11. Стандарты информационной безопасности. Материалы Гостехкомиссии России
12. Классификация компьютерных преступлений по кодификатору Интерпола.
13. Криптография. Основные термины и определения. Задачи криптографии.
14. Этапы развития криптографии
15. Стеганография
16. Шифрование данных. Основные термины и определения. Классификация алгоритмов шифрования.
17. Роторные машины.
18. Американский стандарт шифрования DES.
19. Режимы работы алгоритма DES
20. Российский стандарт шифрования ГОСТ 28147-89.
21. Симметричная криптосистема AES
22. Асимметричные системы шифрования. Основной принцип работы. Однонаправленные функ-ции
23. Система шифрования RSA.
24. Хэш-функции. Основные требования и примеры построения.
25. Алгоритм хэширования SHA
26. Электронная цифровая подпись RSA.
27. Генерация ключей
28. Хранение ключей.
29. Алгоритм безопасного распределения ключей Диффи-Хэллмана
30. Сертификаты открытых ключей
31. Протокол Kerberos
32. Технологии аутентификации
33. Защита информации в сети. Семиуровневая модель OSI. Стек TCP/IP
34. Протокол IPSec. Режимы работы
35. Протокол IPSec. Стратегия безопасности
36. Защита информации в сети. Протокол SSL/TLS
37. Защита информации на прикладном уровне. Протокол PGP
38. Защита информации на прикладном уровне. Протокол S/MIME
39. Система отслеживания вторжений
40. Схемы идентификации и аутентификации. Одно- и многофакторная аутентификация. Система разграничения доступа к информации в компьютерной системе.
41. Аппаратные и программно-аппаратные средства криптозащиты данных.
42. Классификация вирусов. Применение антивирусных программ.

В филиале используется система с традиционной шкалой оценок – «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», «зачтено», «не зачтено» (далее - пятибалльная система).

Форма промежуточной аттестации по настоящей дисциплине – **экзамен во 2 семестре.**

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.

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
	Компетенции на уровне «пороговый», закреплённые за дисциплиной, не сформированы.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебное и учебно-лабораторное оборудование

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.

Учебная аудитория для лабораторных работ, выполняемых в компьютерном классе, оснащенная: специализированной мебелью; доской аудиторной; персональными компьютерами с подключением к сети "Интернет" и доступом в ЭИОС филиала.

Для самостоятельной работы обучающихся по дисциплине используется помещение для самостоятельной работы обучающихся, оснащенное: специализированной мебелью; доской аудиторной; персональным компьютерами с подключением к сети "Интернет" и доступом в ЭИОС филиала.

Программное обеспечение (Операционная система OS Windows, офисный пакет Microsoft Office, Microsoft Visual Studio 2019 Community, Draw.io)

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. Краковский, Ю. М. Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. – 3-е изд., перераб. – Санкт-Петербург : Лань, 2021. – 236 с. – ISBN 978-5-8114-5632-1. URL: https://e.lanbook.com/book/156401.

2. Нестеров, С. А. Основы информационной безопасности: учебник для вузов / С. А. Нестеров. – Санкт-Петербург: Лань, 2021. – 324 с. – ISBN 978-5-8114-6738-9. URL: https://e.lanbook.com/book/165837.

3. Никифоров, С. Н. Методы защиты информации. Защищенные сети: учебное пособие для вузов / С. Н. Никифоров. – 2-е изд., стер. – Санкт-Петербург: Лань, 2021. – 96 с. — ISBN 978-5-8114-8123-1. URL: https://e.lanbook.com/book/171868.

4. Чупин, А. В. Интеллектуальные системы автоматизированного управления: учебное пособие / А. В. Чупин. – Кемерово: КемГУ, 2016. – 108 с. – ISBN 978-5-89289-951-2. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/102654.

Дополнительная литература.

1. Трофимов, В. Б. Интеллектуальные автоматизированные системы управления технологическими объектами: учебно-практическое пособие / В. Б. Трофимов, С. М. Кулаков. – Москва; Вологда: Инфра-Инженерия, 2016. – 232 с. URL: https://biblioclub.ru/index.php?page=book&id=444175.

2. Волкова, Т. В. Проектирование компонентов автоматизированных систем в примерах: учебное пособие / Т. В. Волкова, Е. Н. Чернопрудова. – Оренбург : Оренбургский государственный университет, 2017. – 178 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=481817.

Список авторских методических разработок.

Малашенкова И.В., Панкратова Е.А., Федулова С.А. Методические указания к лабораторным работам по дисциплине «Технологии обеспечения информационной безопасности»: (для студентов направления 10.04.01 «Информационная безопасность») / И.В. Малашенкова, Е.А. Панкратова, С.А. Федулова ; филиал ФГБОУ ВО «НИУ»МЭИ» в г. Смоленске .– Смоленск : [б. и.], 2019 .– 107, [1] с. : ил., табл. – Библиогр.: с. 107 – 104.55.

Малашенкова И.В., Панкратова Е.А., Федулова С.А. Методические указания по выполнению курсовой работы по дисциплине «Технология обеспечения информационной безопасности»: (для студентов направления 10.04.01 «Информационная безопасность») / И.В. Малашенкова, Е.А. Панкратова, С.А.; филиал ФГБОУ ВО «НИУ»МЭИ» в г. Смоленске .— Смоленск : [б. и.], 2019 .– 7, [1] с. – Библиогр.: с. 7 – 10.91.

Федулов Я.А. Комплект мультимедийных презентаций к лекциям по дисциплине «Технологии обеспечения информационной безопасности» (расположен в ЭИОС филиала и передается обучающимся на 1-й лекции для подготовки к лекциям и самостоятельного изучения дисциплины).

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