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
«11» 10 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ

(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: 2022

Смоленск

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:

канд. экон. наук, доц. _____ _____Д.Ю. Шутова_____
подпись ФИО

«28» _____09____ 2021 г.

Программа обсуждена и одобрена на заседании кафедры информационных технологий в экономике и управлении
«29» ____09___ 2021 г., протокол № 1

Заведующий кафедрой информационных технологий в экономике и управлении:

_____ __д-р техн. наук, проф._М.И. Дли_____
подпись ФИО

«08» _____10____ 2021 г.

Согласовано:

Заведующий кафедрой вычислительной техники:

____ _____ __д-р техн. наук, проф._А.С. Федулов_____
подпись ФИО

«08» _____10____ 2021 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» _____10____ 2021 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является подготовка обучающихся к решению задач профессиональной деятельности организационно-управленческого типа в области защиты информации по направлению подготовки 10.04.01 Информационная безопасность (магистерская программа: Безопасность автоматизированных систем) посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС и установленных программой магистратуры на основе профессиональных стандартов, в части представленных ниже знаний, умений и навыков.

Задачи дисциплины: сформировать общее понимание проблематики, целей и задач обеспечения безопасности веб-приложений; знание современных технологий программирования (структурное, модульное программирование); научить разрабатывать требования по защите, формирует политики безопасности компьютерных систем и сетей; сформировать умение проведения анализа безопасности компьютерных систем и сетей.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина Безопасность веб-приложений относится *к части, формируемой участниками образовательных отношений.*

Для изучения данной дисциплины необходимы знания, умения и навыки, формируемые предшествующей дисциплиной:

Б1.В.01 Организационно-правовые механизмы обеспечения информационной безопасности
Б1.В.04 Информационная безопасность компьютерных сетей
Б1.В.07 Технические средства защиты информации
Б1.В.ДВ.02.01 Комплексная защита корпоративной информации
Б1.В.ДВ.02.02 Аудит информационной безопасности

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

Б2.В.02 (П) Проектно-технологическая практика
Б2.В.03 (П) Преддипломная практика
Б3.01 Подготовка к защите и защита выпускной квалификационной работы

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины направлено на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОП ВО по данному направлению подготовки:

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

Компетенция	Индикаторы достижения компетенций	Результаты обучения
ПК-3 Способен управлять безопасностью	ПК-3.1 Проводит анализ безопасности компьютерных систем и сетей	Знать: отечественные и зарубежные стандарты информационной безопасности.

компьютерных систем и сетей		Уметь: формировать функциональные требования к средствам защиты web-приложения от внутренних и внешних угроз. Владеть: навыками разработки структуры системы информационной защиты web-приложений
	ПК-3.2 Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей	Знать: актуальные методы анализа защищенности программных систем; - актуальные методологии разработки программного обеспечения с учетом требований по безопасному функционированию. Уметь: разрабатывать безопасные (защищенные) сетевые приложения с учетом типичных классов угроз безопасности, характерных для современного интернета; определять модель нарушителя при проектировании нового приложения, выбирать адекватные механизмы обеспечения защищенности приложения при его реализации, опираясь на модель нарушителя; выбирать методы анализа защищенности приложения адекватно этапам жизненного цикла программ и в соответствии с моделью нарушителя; применять методы анализа защищенности, обнаруживать уязвимости различных классов и проверять возможность реализации атак на эти уязвимости Владеть: навыками практического использования различных специальных средств тестирования уязвимостей web-приложения; навыками обнаружения уязвимостей приложений и проведения тестирования приложений на наличие уязвимостей

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Структура дисциплины:

№	Индекс	Наименование	Семестр 3										Семестр 4										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.ДВ.03.01	Безопасность веб-приложений	ЗаО РГР	**144**	86	34	34	18		40	18	4													ЗаО РГР	**144**	86	34	34	18		40	18	4		20	3

ОБОЗНАЧЕНИЯ:
Виды промежуточной аттестации (виды контроля):
Экз - экзамен;
ЗаО - зачет с оценкой;
За – зачет;
Виды работ:
Контакт. – контактная работа обучающихся с преподавателем;
Лек. – лекционные занятия;
Лаб.– лабораторные работы;
Пр. – практические занятия;
КРП – курсовая работа (курсовой проект);
РГР – расчетно-графическая работа (реферат);
СР – самостоятельная работа студентов;
з.е.– объем дисциплины в зачетных единицах.

Содержание дисциплины:

№	Наименование видов занятий и тематик, содержание
1	Лекционные занятия 17 шт. по 2 часа: 1.1 Проблемы безопасности web-приложений 1.2 Технологии безопасной передачи информации в сети Интернет (1 часть) 1.3 Технологии безопасной передачи информации в сети Интернет (1 часть) 1.4 Безопасная разработка web-приложения (1 часть) 1.5 Безопасная разработка web-приложения (2 часть) 1.6 Безопасное развертывание web-приложения (1 часть) 1.7 Безопасное развертывание web-приложения (2 часть) 1.8 Безопасное использование web-приложения (1 часть) 1.9 Безопасное использование web-приложения (2 часть) 1.10 Основы тестирования безопасности web-приложения (1 часть) 1.11 Основы тестирования безопасности web-приложения (2 часть) 1.12 Основные виды Интернет-угроз (1 часть) 1.13 Основные виды Интернет-угроз (2 часть) 1.14 Методы защиты от Интернет-угроз (1 часть) 1.15 Методы защиты от Интернет-угроз (2 часть) 1.16 Подсистемы защиты web-порталов от информационных атак 1.17 Понятие и классификация атак на компьютерные сети
2	Лабораторные работы 8 шт. по 4 часа и 1 шт. – 2 часа: 2.1. Анализ внутренних и внешних угроз информационной безопасности web-приложения 2.2. Разработка проекта по построению системы защиты web-приложения 2.3. Разработка клиентской части модуля безопасности web-приложения 2.4. Разработка серверной части модуля безопасности web-приложения 2.5. Разработка средств защиты базы данных web-приложения 2.6. Нагрузочное тестирование web-приложения 2.7. Исследование web-приложения на уязвимости 2.8. Создание сценариев атаки и защиты web-приложения 2.9. Настройка специального программного обеспечения для мониторинга безопасной работы web-приложений (2 час).
3	Практические занятия 9 шт. по 2 часа: 3.1. Безопасность приложений. Мобильные приложения и их уязвимости. 3.2. Модельный пример – платформа Android. 3.3. Веб-приложения: история и основы технологического стека веб-приложений, архитектура и механизмы безопасности на клиенте, механизмы обеспечения безопасности на сервере. 3.4. Исполнение программ на процессоре, стек, подпрограммы и функции, передача аргументов, возврат значения. Системные вызовы. 3.5. Размещение объектов в памяти: статическое, динамическое, автоматическое. Загрузчик программных модулей. 3.6. Уязвимости, связанные с переполнением буфера. 3.7. Уязвимости, связанные с подменой программных модулей. 3.8. Уязвимости, связанные с некорректной проверкой прав доступа 3.9. Механизмы защиты в современных операционных систем
4	Расчетно-графическая работа «Анализ безопасности веб-приложения и формирование

	предложений по ее улучшению»
5	Самостоятельная работа студентов: 5.1 Задачи информационной безопасности. Конфиденциальность, целостность, доступность данных и программ. Понятие политики безопасности. 5.2 Методы обеспечения информационной безопасности – криптография, модели безопасности, контроль поведения. 5.3 Принципы работы основных веб-технологий: протокола HTTP, механизма реализации сеансов cookies, набора технологий HTML 4 (объектная модель документа + CSS + язык javascript). 5.4 Методы обнаружения и эксплуатации распространенных уязвимостей вебприложений: XSS, SQL injection, CSRF, XXE, SSRF. 5.5 Практические аспекты эксплуатации уязвимостей. Взаимодействие аппаратного обеспечения, ядра ОС, загрузчика, прикладных программ и библиотек. Размещение объектов в памяти. 5.6 Выполнение расчетно-графической работы

Текущий контроль:

Индикаторы достижения компетенции	**Вид текущего контроля**	**Тема**
ПК-3.1 Проводит анализ безопасности компьютерных систем и сетей	Опрос Разбор конкретных ситуаций и групповые дискуссии по темам практических занятий Защита лабораторных работ Проверка выполнения заданий расчетно-графической работы Проверка отчета по расчетно-графической работе	Проблемы безопасности web-приложений Технологии безопасной передачи информации в сети Интернет Безопасная разработка web-приложения Основы тестирования безопасности web-приложения Основные виды Интернет-угроз Методы защиты от Интернет-угроз Подсистемы защиты web-порталов от информационных атак
ПК-3.2 Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей	Опрос Разбор конкретных ситуаций и групповые дискуссии по темам практических занятий Защита лабораторных работ Проверка выполнения заданий расчетно-графической работы Проверка отчета по расчетно-графической работе	Безопасная разработка web-приложения Безопасное развертывание web-приложения Безопасное использование web-приложения Основы тестирования безопасности web-приложения Основные виды Интернет-угроз Методы защиты от Интернет-угроз Подсистемы защиты web-порталов от информационных атак Понятие и классификация атак на компьютерные сети

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	Технологии проведения практических занятий в форме семинара: тематический семинар Технология проблемного обучения на основе анализа ситуаций и имитационных моделей: групповая дискуссия, метод «круглого стола», работа малыми группами, командная работа, анализ-презентация Технология развития критического мышления: учебно-мозговой штурм, интеллектуальная разминка Технология обучения в сотрудничестве (командная, групповая работа)
3	Лабораторная работа	Технология выполнения лабораторных заданий индивидуально Проектная технология Допуск к лабораторной работе
4	Самостоятельная работа студентов (внеаудиторная)	Информационно-коммуникационные технологии (доступ к ЭИОС филиала, к ЭБС филиала, доступ к информационно-методическим материалам по дисциплине)
5	Контроль (промежуточная аттестация: зачет)	Технология устного опроса 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.

Вопросы для защиты лабораторной работы «Анализ внутренних и внешних угроз информационной безопасности web-приложения»

1. Приведите примеры внутренних угроз безопасности web-приложения.
2. Приведите примеры внешних угроз безопасности web-приложения.
3. Опишите основные методы анализа уязвимостей web-приложения.

Вопросы для защиты лабораторной работы «Разработка проекта по построению системы защиты web-приложения»

1. Приведите примеры отечественных и иностранных стандартов информационной безопасности.
2. Опишите безопасный цикл разработки web-приложения.
3. Какие языки программирования используются для разработки web-приложений.

Вопросы для защиты лабораторной работы «Разработка клиентской части модуля безопасности web-приложения»

1. Для чего используется Content Security Policy?
2. Что такое межсетевые запросы?
3. Опишите механизм атаки CRLF-инъенкции, направленной на пользователя web-приложения.

Вопросы для защиты лабораторной работы «Разработка клиентской части модуля безопасности web-приложения»

1. Какие серверные операционные системы чаще всего используют в сети Интернет?
2. Что такое виртуальные хосты в web-серверах Apache и Nginx?
3. Приведите примеры архитектурных анти-паттернов, связанных с безопасностью.

Вопросы для защиты лабораторной работы «Разработка средств защиты базы данных web-приложения»

1. Опишите цикл безопасной обработки данных.
2. Что такое «SQL-инъекция»?
3. Перечислите способы борьбы с SQL-инъекциями.

Вопросы для защиты лабораторной работы «Нагрузочное тестирование web-приложения»

1. Что такое тестирование на проникновение?
2. Для чего нужен балансировщик нагрузки?
3. Влияет ли использование скриптовых языков программирования (например, PHP) на производительность web-сервера?

Вопросы для защиты лабораторной работы «Исследование web-приложения на уязвимости»

1. Что такое межсайтовый скриптинг?
2. Что такое «XML-инъекция»?
3. Что такое инъекции в HTTP-заголовки?

Вопросы для защиты лабораторной работы «Создание сценариев атаки и защиты web-приложения»

1. Поясните суть атак «грубая сила» и «переполнение буфера».
2. Поясните суть атаки «инъекция команд в протоколы электронной почты».
3. Поясните суть атаки «злоупотребление функциональностью».

Вопросы для защиты лабораторной работы «Настройка специального программного обеспечения для мониторинга безопасной работы web-приложений»

1. Как используются защищенные и незащищенные протоколы передачи данных?
2. Приведите примеры антивирусов, используемых для организации безопасности web-

серверов.

3. Опишите возможную митигацию для всех угроз, найденных приложением

Вопросы для опроса на практических занятиях

1. Какие три основных класса угроз безопасности различают в информационных системах, что такое модель нарушителя?
2. Какие виды программных уязвимостей являются актуальными в настоящее время, как реализуются компьютерные атаки с помощью программных уязвимостей, какие существуют подходы к разработке безопасного (защищенного) мобильного приложения?
3. Технологии и инструменты обеспечения информационной безопасности на этапе разработки web-приложения.
4. Технологии и инструменты обеспечения информационной безопасности на этапе тестирования web-приложения.
5. Технологии и инструменты обеспечения информационной безопасности на этапе внедрения web-приложения.
6. Технологии и инструменты обеспечения информационной безопасности на этапе использования web-приложения.
7. Защищенные и незащищенные протоколы передачи данных и их использование.
8. Виды DDoS-атак. Обнаружение DDoS-атак.
9. Причины возникновения уязвимостей типа Injection.
10. Подсистемы защиты web-порталов от информационных атак

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 – *зачет с оценкой в 3-м семестре.*

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

1. Проблемы безопасности web-приложений.
2. Внутренние и внешние угрозы информационной безопасности web-приложения.
3. Технологии безопасной передачи информации в сети Интернет.
4. Жизненный цикл защиты web-приложения.
5. Технологии и средства безопасной разработки web-приложения.
6. Технологии и средства безопасного развертывания web-приложения.
7. Технологии и средства безопасного использования web-приложения.
8. Основы тестирования безопасности web-приложения.
9. Разработка клиентской части модуля безопасности web-приложения.
10. Разработка серверной части модуля безопасности web-приложения.
11. Средства защиты базы данных web-приложения.
12. Основные виды Интернет-угроз и методы защиты от них.
13. Подсистемы защиты web-порталов от информационных атак.
14. Особенности исследования web-приложения на уязвимости.

15. Специальное программное обеспечение для мониторинга безопасной работы web-приложений.

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

Задача №

1. Написать SQL-запрос на получение имени таблиц базы данных и последующее получение данных из найденных таблиц
2. Написать запрос на получение первого символа у второй записи в таблице.

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..

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

Для проведения практических занятий

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

- специализированной мебелью; доской аудиторной; демонстрационным оборудованием: персональным компьютером (ноутбуком); переносным (стационарным) проектором.

Для проведения занятий лабораторного типа

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

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

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

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

Программное обеспечение

При проведении лекционных занятий предусматривается использование программного обеспечения Microsoft Office (презентационный редактор Microsoft Power Point).

При проведении **практических занятий** предусматривается использование программного обеспечения предусматривается использование обучающимися программного обеспечения Microsoft Office: (текстовый редактор Microsoft Word; электронные таблицы Microsoft Excel)

При проведении **лабораторных работ** предусматривается использование программного средства защиты информации Microsoft Office: (текстовый редактор Microsoft Word; электронные таблицы Microsoft Excel; презентационный редактор Microsoft Power Point), PostgreSQL, Apachewebserver, Visio Professional 2019, Secret Net Studio.

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

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 Басыня Е.А. Системное администрирование и информационная безопасность : учебное пособие : / Е.А. Басыня ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=575325

2 Вагин Д.В. Современные технологии разработки веб-приложений : учебное пособие / Д.В. Вагин, Р.В. Петров ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 52 с. : ил. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=573960

3 Малашкевич В.Б. Интернет-программирование : лабораторный практикум / В.Б. Малашкевич ; Поволжский государственный технологический университет. — Йошкар-Ола : ПГТУ, 2017. — 96 с. — Режим доступа: http://biblioclub.ru/index.php?page=book&id=476400.

Дополнительная литература.

1 Брылёва А.А. Программные средства создания интернет-приложений : учебное пособие / А.А. Брылёва. – Минск : РИПО, 2019. – 381 с. : ил., табл. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=600089

2 Савельева Н.В. Язык программирования PHP [Электронный ресурс]. — 2-е изд., испр. — Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 330 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=428975.

3 Вальке А.А. Электронные средства сбора и обработки информации : учебное пособие / А.А. Вальке, В.А. Захаренко ; Минобрнауки России, Омский государственный технический

университет. — Омск : Издательство ОмГТУ, 2017. — 112 с. — Режим доступа: http://biblioclub.ru/index.php?page=book&id=493448

4 Булыгина О.В. Методические указания по выполнению расчетно-графической работы по дисциплине «Безопасность веб-приложений» [Электронный ресурс]: электронные методические указания для студентов, обучающихся по направлению 10.04.01 «Информационная безопасность» / Булыгина О.В. – Электрон. дан. – Смоленск: РИО филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2019.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет» необходимых для освоения дисциплины

1 Справочная правовая система Консультант плюс [электронный ресурс] — Режим доступа : http://www.consultant.ru/online/.

2 Официальный сайт Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) [электронный ресурс] — Режим доступа : http://government.ru/department/387/events/.

3 Официальный сайт Росстата [электронный ресурс] — Режим доступа : www.gks.ru/.

4 20 интернет-ресурсов для специалистов по информационной безопасности // официальный сайт компании «ГЕОЛАЙН Технологии» [электронный ресурс] — Режим доступа : http://geoline-tech.com/top-20-sites-about-information-security/.

5 Полезные сайты и инструменты// Информационная безопасность. Практика информационной безопасности [электронный ресурс] — Режим доступа : http://dorlov.blogspot.com/p/blog-page_3151.html.

6 Информационная безопасность [электронный ресурс] — Режим доступа : http://www.securrity.ru/.

7 30 ресурсов по безопасности, которые точно пригодятся [электронный ресурс] — Режим доступа : https://proglib.io/p/information-security-guide/

8 Информационная безопасность. Защита данных // habr - веб-сайт в формате коллективного блога с элементами новостного сайта [электронный ресурс] — Режим доступа : https://habr.com/ru/hub/infosecurity/.

9 База Знаний Клуба Информационной безопасности [электронный ресурс] — Режим доступа : http://wiki.informationsecurity.club/doku.php/main.

10 Информационная безопасность. Защита данных [электронный ресурс] — Режим доступа : http://all-ib.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