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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Владелец: Федулов Александр Сергеевич
Сертификат: 5A022291D0DE01CCADCB2B81371C7969
Действителен: 06.05.2025 - 30.07.2026

УТВЕРЖДАЮ
Зам. директора филиала ФГБОУ ВО
«НИУ «МЭИ» в г. Смоленске
канд. техн. наук, доцент
_____ В.В. Рожков
«06» 03 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ

(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: 09.03.03 «Прикладная информатика»

Профиль «Безопасность экономических информационных систем»

Уровень высшего образования: бакалавриат

Нормативный срок обучения: 4 года

Форма обучения: очная

Год набора: 2026

Смоленск

Программа составлена с учетом ОС ВО по направлению подготовки 09.03.03 Прикладная информатика, утвержденного ректором ФГБОУ ВО «НИУ «МЭИ» Н.Д. Рогалевым 20.12.2023.

Программу составил:

канд. экон. наук, доц. _____ О.В. Булыгина
подпись ФИО

«17» февраля 2026 г.

Программа обсуждена и одобрена на заседании кафедры информационных технологий в экономике и управлении
«18» февраля 2026 г., протокол № 6

Заведующий кафедрой информационных технологий в экономике и управлении:

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

«05» марта 2026 г.

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Ответственный в филиале по работе
с ЛОВЗ и инвалидами

_____ Е.В. Зуева
подпись ФИО

«05» марта 2026 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является подготовка обучающихся к решению задач профессиональной деятельности научно-исследовательского и организационно-управленческого типов в области информационных и коммуникационных технологий по направлению подготовки 09.03.03 Прикладная информатика (профиль подготовки: Безопасность экономических информационных систем) посредством обеспечения этапов формирования компетенций, предусмотренных ОС и установленных программой бакалавриата на основе профессиональных стандартов, в части представленных ниже знаний, умений и навыков.

Задачи дисциплины: сформировать общее понимание проблематики, целей и задач обеспечения безопасности веб-приложений; научить разрабатывать требования по защите, формирует политики безопасности веб-приложений; сформировать умение проведения мониторинга и аудита защищенности информации в автоматизированных информационных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

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

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

Б1.О.03 Философия
Б1.О.06 Информационные технологии
Б1.О.07 Программные средства для экономико-математических расчетов
Б1.О.08 Учет и анализ
Б1.О.09 Вычислительные системы, сети и телекоммуникации
Б1.О.10 Управление проектами
Б1.О.11 Операционные системы
Б1.О.13 Правоведение
Б1.О.14 Теория систем и системный анализ
Б1.О.15 Алгоритмизация и программирование
Б1.О.16 Базы данных
Б1.О.17 Разработка и стандартизация программных средств и информационных технологий
Б1.В.01 Экономическая информатика
Б1.В.02 Экономическая статистика
Б1.В.03 Организационные основы информационной безопасности
Б1.В.04 Реинжиниринг и управление бизнес-процессами
Б1.В.05 Менеджмент
Б1.В.07 Маркетинг
Б1.В.08 Финансовый менеджмент
Б1.В.09 Аудит информационной безопасности
Б1.В.ДВ.01.01 Цифровая экономика
Б1.В.ДВ.01.02 Информационная логистика
Б2.В.01(У) Ознакомительная практика

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

Б1.В.11 Управление инцидентами информационной безопасности организации
Б1.В.12 Основы экономической безопасности бизнеса
Б1.В.13 Проектирование информационных систем

Б1.В.14 Информационная безопасность телекоммуникационных систем и сетей связи
Б1.В.16 Программная инженерия
Б1.В.18 Контроллинг
Б1.В.ДВ.02.01 Управление инновациями и инвестициями
Б1.В.ДВ.02.02 Корпоративные информационные системы
Б1.В.ДВ.03.01 Интеллектуальные информационные системы
Б1.В.ДВ.03.02 Мировые информационные ресурсы
Б1.В.ДВ.04.01 Стратегический анализ и стратегии информационной безопасности
Б1.В.ДВ.04.02 Информационная бизнес-аналитика
Б2.В.02(П) Технологическая (проектно-технологическая) практика
Б2.В.03(Н) Научно-исследовательская работа
Б2.В.04(Пд) Преддипломная практика
Б3.01 Подготовка к защите и защита выпускной квалификационной работы

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

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

Компетенция	Индикаторы достижения компетенций	Результаты обучения
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Анализирует задачу, выделяя ее базовые составляющие	Знает: роли, функции и задачи, решаемые в рамках организации безопасности веб-приложений. Уметь: сравнивать и анализировать альтернативные варианты организации безопасности веб-приложений; Владеть: методами анализа эффективности предложены методов организации безопасности веб-приложений.
	УК-1.2 Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи	Умеет: использовать и анализировать информацию, как средство достижения поставленных целей; решать поставленные задачи; Владеет: методиками выбирать рациональные способы организации безопасности веб-приложений.
	УК-1.3 Осуществляет поиск информации для решения поставленной задачи по различным типам запросов	Знает: способы поиска необходимой для достижения поставленных целей и решения поставленных задач информации; Умеет: искать информацию, необходимую для достижения поставленных целей и решения поставленных задач;

	УК-1.4 При обработке информации отличает факты от мнений, интерпретаций, оценок, формирует собственные мнения и суждения, аргументирует свои выводы и точку зрения	Знает: отличия фактов от мнений Умеет: обрабатывать полученную информацию, умеет сформулировать собственное мнение на основании полученной информации Владеет: навыками обработки информации.
	УК-1.5 Рассматривает и предлагает возможные варианты решения поставленной задачи, оценивая их достоинства и недостатки	Умеет: формулировать задачи проекта, способен предложить несколько вариантов решения и оценить их достоинства и недостатки Владеет: навыками оценки предложенных решений, а так же методами оценки рисковых событий
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Определяет круг задач в рамках поставленной цели проекта, определяет связи между ними	Знает: правила формулирования целей и задач; Умеет: выявлять информационные потребности и разрабатывать требования к веб-приложениям с точки зрения обеспечения информационной безопасности Владеет: практическими навыками формулировки целей и задач проекта по обеспечению информационной безопасности веб-приложений.
	УК-2.2 Предлагает способы решения поставленных задач и ожидаемые результаты; оценивает предложенные способы с точки зрения соответствия цели проекта	Знает: правила формулирования целей и задач проекта по обеспечению информационной безопасности веб-приложения; Умеет: определять и формулировать цели и задачи проекта по обеспечению информационной безопасности веб-приложения; Владеет: навыками планирования и организации выполнения работ по проекту обеспечения информационной безопасности веб-приложения.
	УК-2.3 Планирует реализацию задач в зоне своей ответственности с учетом имеющихся ресурсов и ограничений, действующих правовых норм	Знает: основы правовых знаний в области обеспечения информационной безопасности; Умеет: использовать основы правовых знаний в области информационной безопасности Владеет: правовыми нормами реализации профессиональной деятельности в сфере информационной безопасности
	УК-2.4 Выполняет задачи в зоне своей ответственности в соответствии с запланированными результатами и точками контроля, при необходимости корректирует способы решения задач	Знает: основные методы обеспечения информационной безопасности веб-приложений Умеет: определять уровень защищенности веб-приложения и предлагать решения по совершенствованию информационной безопасности Владеет: навыками построения системы информационной безопасности

		веб-приложения
	УК-2.5 Представляет результаты проекта, предлагает возможности их использования и/или совершенствования	Знает: основные способы представления результатов, методы анализа полученных результатов. Умеет: применять методы анализа полученных результатов и делать выводы. Владеет: навыками представления полученных результатов
ПК-6. Способен внедрять системы защиты информации автоматизированных систем и обеспечить защиту информации в процессе их эксплуатации	ПК-6.1 Проводит диагностику систем защиты информации автоматизированных информационных систем	Знает: актуальные методы анализа защищенности программных систем; Умеет: 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; Владеет: навыками практического использования различных специальных средств тестирования уязвимостей web-приложения.
	ПК-6.2 Осуществляет администрирование систем защиты информации автоматизированных информационных систем	Знает: актуальные методологии разработки программного обеспечения с учетом требований по безопасному функционированию. Умеет: 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 Владеет: навыками обнаружения уязвимостей приложений и проведения тестирования приложений на наличие уязвимостей
	ПК-6.4 Осуществляет мониторинг и аудит защищенности информации в автоматизированных информационных систем	Знает: отечественные и зарубежные стандарты информационной безопасности. Умеет: формировать функциональные требования к средствам защиты web-приложения от внутренних и внешних угроз. Владеет: навыками разработки структуры системы информационной защиты web-приложений
ПК-7. Способен проводить научно-исследовательские и	ПК-7.1 Проводит маркетинговые исследования на рынке программно-технических средств, информа-	Знает: существующие программно-технические средства для обеспечения информационной безопасности Умеет: выбирать необходимые про-

опытно-конструкторские разработки по отдельным разделам темы	ционных продуктов и услуг	граммно-технические средства для обеспечения информационной безопасности Владеет: навыками анализа и выбора необходимых программно-технические средства для обеспечения информационной безопасности
	ПК-7.2 Собирает, обрабатывает, анализирует и обобщает передовой отечественный и международный опыт в соответствующей области исследований	Знает: методы анализа и обобщения отечественного и международного опыта в области обеспечения информационной безопасности Умеет: применять методы анализа и обобщения отечественного и международного опыта в области обеспечения информационной безопасности Владеет: навыками сбора, анализа и обработки информации в области обеспечения информационной безопасности
	ПК-7.3 Собирает, обрабатывает, анализирует, обобщает, оформляет и осуществляет презентацию результатов исследований	Знает: способы оформления результатов анализа и обобщения отечественного и международного опыта в области обеспечения информационной безопасности Умеет: применять способы оформления результатов анализа и обобщения отечественного и международного опыта в области обеспечения информационной безопасности Владеет: навыками представления результатов исследований

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Структура дисциплины:

№	Индекс	Наименование	Семестр 5											Семестр 6											Итого за курс											Каф.	Семестры
			Контроль	Академических часов								з.е.	Недель	Контроль	Академических часов								з.е.	Недель	Контроль	Академических часов								з.е.	Недель		
				Всего	Конт такт.	Лек	Лаб	Пр	КРП	СР	Конт роль				Всего	Конт такт.	Лек	Лаб	Пр	КРП	СР	Конт роль				Всего	Конт такт.	Лек	Лаб	Пр	КРП	СР	Конт роль	Всего			
7	Б1.В.10	Информационная безопасность веб-приложений												Эк КР	**180**	68	30	30		8	76	36	5		Эк КР	**180**	68	30	30		8	76	36	5		20	6

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 15 шт. по 2 часа: Тема 1 Основы информационной безопасности web-технологий 1.1 Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. (часть 1) 1.2 Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. (часть 2) 1.3 Проблемы безопасности web-приложений 1.4 Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия. (часть 1) 1.5 Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия. (часть 2) Тема 2 Жизненный цикл защиты web-приложения 1.6. Безопасная разработка web-приложения. (часть 1) 1.7. Безопасная разработка web-приложения. (часть 2) 1.8. Безопасное развертывание web-приложения 1.9 Безопасное использование web-приложения 1.10 Основы тестирования безопасности web-приложения Тема 3 Виды Интернет-угроз и способы защиты от них 1.11 Основные виды Интернет-угроз (часть 1) 1.12 Основные виды Интернет-угроз (часть 2) 1.13 Методы защиты от Интернет-угроз (часть1) 1.14 Методы защиты от Интернет-угроз (часть2) 1.15 Подсистемы защиты web-порталов от информационных атак
2	Лабораторные работы 7 шт. по 4 часа и 1 шт. – 2 часа: 2.1 Архитектура веб-приложений 2.2 Специфика работы веб-приложений 2.3 Разработка веб-приложения. Техническое задание 2.4 Разработка веб-приложения.Разработка прототипов станиц. Разработка макета средствами HTML 2.5 Разработка веб-приложения. Дизайн. Принципы разработки пользовательского интерфейса веб-приложения. 2.6 Организация взаимодействия клиентской и серверной части веб-приложения 2.7 Организация взаимодействия веб-приложения с базами данных 2.8 Анализ внутренних и внешних угроз информационной безопасности web-приложения 2.9 Исследование web-приложения на уязвимости (2 час)
3	Консультации по курсовой работе: 4 шт. по 2 часа
4	Курсовая работа «Поиск и ликвидация уязвимостей разработанного Веб-приложения»
5	Самостоятельная работа студентов: 4.1 Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. 4.2 Кражи паролей в сети Интернет. Способы защиты. 4.3 Вид взлома «Взлом электронной почты». Способы защиты. 4.4 Кража FTP-паролей. Способы защиты.

	4.5. Вид взлома «Загрузка файлов». Способы защиты. 4.6 . Вид взлома «Register Globals». Способы защиты 4.7 Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз.

Текущий контроль:

Индикаторы достижения компетенции	Вид текущего контроля	Тема
УК-1.1 Анализирует задачу, выделяя ее базовые составляющие	Защита лабораторной (лабораторных) работ	Тема 1 Основы информационной безопасности web-технологий
УК-1.2 Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи	Опрос Защита лабораторной (лабораторных) работ Проверка выполнения заданий курсовой работы Проверка отчета по расчетно-графической работе	Тема 1 Основы информационной безопасности web-технологий
УК-1.3 Осуществляет поиск информации для решения поставленной задачи по различным типам запросов	Опрос Защита лабораторной (лабораторных) работ Проверка выполнения заданий курсовой работы Проверка отчета по расчетно-графической работе	Тема 1 Основы информационной безопасности web-технологий Тема 2 Жизненный цикл защиты web-приложения Тема 3 Виды Интернет-угроз и способы защиты от них
УК-1.4 При обработке информации отличает факты от мнений, интерпретаций, оценок, формирует собственные мнения и суждения, аргументирует свои выводы и точку зрения	Опрос Защита лабораторной (лабораторных) работ Проверка выполнения заданий курсовой работы Проверка отчета по расчетно-графической работе	Тема 1 Основы информационной безопасности web-технологий Тема 3 Виды Интернет-угроз и способы защиты от них
УК-1.5 Рассматривает и предлагает возможные варианты решения поставленной задачи, оценивая их достоинства и недостатки	Опрос Защита лабораторной (лабораторных) работ Проверка выполнения заданий курсовой работы Проверка отчета по расчетно-графической работе	Тема 1 Основы информационной безопасности web-технологий Тема 2 Жизненный цикл защиты web-приложения Тема 3 Виды Интернет-угроз и способы защиты от них
УК-2.1 Определяет круг задач в рамках поставленной цели проекта, определяет связи между ними	Опрос Защита лабораторной (лабораторных) работ Проверка выполнения заданий курсовой работы Проверка отчета по расчетно-графической работе	Тема 1 Основы информационной безопасности web-технологий Тема 2 Жизненный цикл защиты web-приложения
УК-2.2 Предлагает способы решения поставленных задач и ожидаемые результаты; оцени-	Опрос Защита лабораторной (лабораторных) работ	Тема 1 Основы информационной безопасности web-технологий

вает предложенные способы с точки зрения соответствия цели проекта	Проверка выполнения заданий курсовой работы Проверка отчета по расчетно-графической работе	Тема 2 Жизненный цикл защиты web-приложения
УК-2.3 Планирует реализацию задач в зоне своей ответственности с учетом имеющихся ресурсов и ограничений, действующих правовых норм	Опрос Защита лабораторной (лабораторных) работ Проверка выполнения заданий курсовой работы Проверка отчета по расчетно-графической работе	Тема 1 Основы информационной безопасности web-технологий
УК-2.4 Выполняет задачи в зоне своей ответственности в соответствии с запланированными результатами и точками контроля, при необходимости корректирует способы решения задач	Опрос Защита лабораторной (лабораторных) работ Проверка выполнения заданий курсовой работы Проверка отчета по расчетно-графической работе	Тема 2 Жизненный цикл защиты web-приложения Тема 3 Виды Интернет-угроз и способы защиты от них
УК-2.5 Представляет результаты проекта, предлагает возможности их использования и/или совершенствования	Опрос Защита лабораторной (лабораторных) работ Проверка выполнения заданий курсовой работы Проверка отчета по расчетно-графической работе	Тема 2 Жизненный цикл защиты web-приложения Тема 3 Виды Интернет-угроз и способы защиты от них
ПК-6.1 Проводит диагностику систем защиты информации автоматизированных информационных систем	Опрос Защита лабораторной (лабораторных) работ Проверка выполнения заданий курсовой работы Проверка отчета по расчетно-графической работе	Тема 2 Жизненный цикл защиты web-приложения Тема 3 Виды Интернет-угроз и способы защиты от них
ПК-6.2 Осуществляет администрирование систем защиты информации автоматизированных информационных систем	Опрос Защита лабораторной (лабораторных) работ Проверка выполнения заданий курсовой работы Проверка отчета по расчетно-графической работе	Тема 2 Жизненный цикл защиты web-приложения Тема 3 Виды Интернет-угроз и способы защиты от них
ПК-6.4 Осуществляет мониторинг и аудит защищенности информации в автоматизированных информационных системах	Опрос Защита лабораторной (лабораторных) работ Проверка выполнения заданий курсовой работы Проверка отчета по расчетно-графической работе	Тема 2 Жизненный цикл защиты web-приложения Тема 3 Виды Интернет-угроз и способы защиты от них
ПК-7.1 Проводит маркетинговые исследования на рынке программно-технических средств, информационных	Защита лабораторной (лабораторных) работ Проверка выполнения заданий курсовой работы	Тема 1 Основы информационной безопасности web-технологий Тема 2 Жизненный цикл защи-

продуктов и услуг		ты web-приложения Тема 3 Виды Интернет-угроз и способы защиты от них
ПК-7.2 Собирает, обрабатывает, анализирует и обобщает передовой отечественный и международный опыт в соответствующей области исследований	Защита лабораторной (лабораторных) работ Проверка выполнения заданий курсовой работы	Тема 1 Основы информационной безопасности web-технологий Тема 2 Жизненный цикл защиты web-приложения Тема 3 Виды Интернет-угроз и способы защиты от них
ПК-7.3 Собирает, обрабатывает, анализирует, обобщает, оформляет и осуществляет презентацию результатов исследований	Защита лабораторной (лабораторных) работ Проверка выполнения заданий курсовой работы	Тема 1 Основы информационной безопасности web-технологий Тема 2 Жизненный цикл защиты web-приложения Тема 3 Виды Интернет-угроз и способы защиты от них

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)
2	Лабораторная работа	Технология выполнения лабораторных заданий индивидуально
3	Самостоятельная работа студентов (внеаудиторная)	Информационно-коммуникационные технологии (доступ к ЭИОС филиала, к ЭБС филиала, доступ к информационно-методическим материалам по дисциплине)
4	Контроль (экзамен)	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.

Оценочные средства текущего контроля

Вопросы для защиты лабораторной работы «Разработка веб-приложения.Разработка прототипов станиц. Разработка макета средствами HTML».

1. Опишите состав и структуру веб-приложения
2. Что такое HTML? Что такое гипертекстовый документ?
3. Является ли язык HTML языком программирования?
4. Укажите основные достоинства и недостатки языка HTML

Вопросы для защиты лабораторных работ «Организация взаимодействия клиентской и серверной части веб-приложения» и «Организация взаимодействия веб-приложения с базами данных»

1. Описать наиболее популярные языки Web-программирования.
2. Достоинства и недостатки языков Web-программирования.
3. Деление на группы языков Web-программирования: клиентские и серверные. Опишите, как обрабатываются скрипты на сервере. Примеры языков каждой группы.
4. Язык Web-программирования PHP. Достоинства, недостатки.
5. Дать характеристику каждого этапа разработки web-приложений

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

1. Какие угрозы были выявлены в результате анализа информационной безопасности?
2. Какие способы улучшения системы информационной безопасности вы можете предложить?
3. Какие угрозы относятся к внешним а какие к внутренним?
4. Опишите основные требования к системы защиты web-приложения
5. Какие цели создаваемой системы безопасности? Какие задачи необходимо решить для достижения поставленных целей?

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

1. Объясните, какой метод передачи информации используют при передаче конфиденциальной информации.
2. Поясните, что означает знак «+», который появляется в адресной строке браузера при определенном типе протокола обмена данными
3. Какие уязвимости были выявлены в ходе анализа веб-приложения? Каким образом моно их устранить?

Вопросы для защиты курсовой работы

1. Основные принципы построения безопасных веб-приложений
2. Понятие безопасности приложений и классификация опасностей
3. Источники угроз информационной безопасности и меры по их предотвращению
4. Регламенты и методы разработки безопасных веб-приложений
5. Безопасная аутентификация и авторизация.
6. Повышение привилегий и общая отказоустойчивость системы
7. Проверка корректности данных, вводимых пользователем.
8. Общие сведения о тестировании web-приложений: верификация, валидация, разновидности тестирования: функциональное, нагрузочное и стрессовое тестирование.
9. Сетевые протоколы, сетевой трафик.
10. Отображение элементов веб-приложения в различных браузерах.

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 6-м семестре.*

Оценочные средства промежуточной аттестации

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

1. Задачи информационной безопасности.
2. Конфиденциальность, целостность, доступность данных и программ. Понятие политики безопасности.
3. Методы обеспечения информационной безопасности – криптография, модели безопасности, контроль поведения.
4. Принципы работы основных веб-технологий: протокола HTTP, механизма реализации сеансов cookies, набора технологий HTML (объектная модель документа + CSS + язык javascript).
5. Методы обнаружения и эксплуатации распространенных уязвимостей вебприложений: XSS, SQL injection, CSRF, XXE, SSRF.
6. Практические аспекты эксплуатации уязвимостей. Взаимодействие аппаратного обеспечения, ядра ОС, загрузчика, прикладных программ и библиотек. Размещение объектов в памяти.
7. Уязвимости, связанные с переполнением буфера. Варианты.
8. Уязвимости, связанные с подменой программных модулей. Уязвимости, связанные с некорректной проверкой прав доступа, TOCTOU. 8. Уязвимости переполнения кучи.
9. Режимы шифрования в блочных шифрах.
10. Алгоритм RSA.
11. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.
12. Основные понятия информационной безопасности.
13. Персональные данные и их защита.
14. Информационные угрозы, их виды и причины возникновения.
15. Что такое «хостинг»? Какие виды хостингов Вы знаете? В чем их принципиальные различия? Расскажите про «подводные камни»?
16. Что такое доменное имя? Что Вы знаете про доменные имена? Что такое DNS? Что такое DNS-сервер? Зачем нужны DNS сервера, как они настраиваются?
17. Что такое TCP/IP, как он работает, расскажите?
18. Что такое HTTP и HTTPS, как они работают? Что такое ssl сертификаты? Зачем они нужны?
19. Что такое HTML, HTML5, CSS, PHP, JavaScript, jQuery? В чем принципиальные различия между PHP и JavaScript ?
20. Что такое MySQL? Для чего нужен MySQL? Как работает MySQL? Что такое phpMyAdmin? Для чего нужен phpMyAdmin?
21. Как происходят кражи паролей в сети Интернет? Способы защиты?
22. Вид взлома «Загрузка файлов». Как используют злоумышленники? Способы защиты?
23. Вид взлома «Register Globals». Как используют злоумышленники? Способы защиты?

24. Какие антивирусы для организации безопасности веб-серверов Вы знаете? Назовите их.
25. Зачем нужны сканеры уязвимостей веб-сервера или сайта. Какие Вы знаете? Какие функции они Выполняют?

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

Дано веб-приложение с несколькими функциями, авторизацией пользователей, в котором функции доступны после успешной авторизации. В приложение искусственно внесены уязвимости. Требуется найти эти уязвимости и реализовать успешную атаку на каждую из них. Подтверждением успеха является доступ к секретной строке, которая доступна только с помощью успешной атаки на уязвимость.

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

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

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

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
	говый».
«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 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.

Для проведения консультаций по курсовой работе

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

- специализированной мебелью; доской аудиторной

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

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

8. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ

С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

для глухих и слабослышащих:

- лекции оформляются в виде электронного документа;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере;
- используется специальная учебная аудитория для лиц с ЛОВЗ – ауд. 106 главного учебного корпуса по адресу 214013, г. Смоленск, Энергетический пр-д, д.1, здание энергетического института (основной корпус).

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены филиалом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается **доступ к информационным и библиографическим ресурсам в сети Интернет** для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

для обучающихся с нарушениями опорно-двигательного аппарата:
- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература.

1 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

Список авторских методических разработок.

1 Шутова Д.Ю. Методические указания по выполнению лабораторных работ по дисциплине "Информационная безопасность веб-приложений" : по направлению 09.03.03 "Прикладная информатика" (профиль "Безопасность экономических информационных систем") / Д.Ю. Шутова, М.В. Черновалова ; Министерство науки и высшего образования Российской Федерации, Филиал ФГБОУ ВО "НИУ "МЭИ" в г. Смоленске, Кафедра Информационных технологий в экономике и управлении .— Смоленск : [б. и.], 2021 .— 19 с. : табл. ; 1 файл: 289 Кб .— Загл. с титул. экрана .— Библиогр.: с. 16 .— Системные требования: Acrobat Reader .— Электрон. копия представлена на сайте Библиотеки вуза .— б.ц. — <URL:http://lib.sbmpei.ru/file/upload/L_121.pdf>

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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