Федеральное государственное автономное образовательное учреждение высшего образования
"Самарский государственный экономический университет"

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «БЕЗОПАСНОСТЬ WEB-ПРИЛОЖЕНИЙ»

Уровень высшего образования: бакалавриат

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль)подготовки: Прикладная информатика и защита информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очно-заочная

Год набора (приема на обучение): 2026

Срок получения образования: 4 года 6 месяца(-ев)

Объем: в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

г. Самара, 2026

Разработчики:
Не имеет Колотилина М. А.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом Минобрнауки от 19.09.2017 № 922, с учетом трудовых функций профессиональных стандартов: "Специалист по информационным системам", утвержден приказом Минтруда России от 13.07.2023 № 586н; "Руководитель проектов в области информационных технологий", утвержден приказом Минтруда России от 27.04.2023 № 369н; "Системный аналитик", утвержден приказом Минтруда России от 27.04.2023 № 367н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	Кафедра прикладной информатики	Заведующий кафедрой, руководитель подразделения, реализующего ОП	Ермолина Л. В.	Рассмотрено	21.05.2026, № 9

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование теоретических знаний и практических навыков по выявлению, анализу и устранению уязвимостей веб-приложений, а также внедрению защитных механизмов для обеспечения безопасности на всех этапах жизненного цикла разработки.

Задачи изучения дисциплины:

- Изучить архитектуру веб-приложений, модели угроз и основные виды атак (OWASP Top 10), включая инъекции, XSS, CSRF и нарушение аутентификации.;
- Освоить методы статического и динамического анализа безопасности веб-приложений, а также инструменты тестирования на проникновение (Burp Suite, OWASP ZAP).;
- Сформировать навыки разработки защищённого кода, внедрения средств защиты (WAF, шифрование, контроль доступа) и мониторинга безопасности веб-приложений в процессе эксплуатации..

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-1 Способен к разработке прототипов ИС и к созданию программного кода ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы

ПК-1.2 Создает программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления

Знать:

ПК-1.2/Зн1 Основные виды уязвимостей веб-приложений (OWASP Top 10), принципы безопасного программирования (валидация ввода, кодирование вывода, параметризация запросов), методы защиты от инъекций, XSS, CSRF и нарушения аутентификации.

Уметь:

ПК-1.2/Ум1 Создавать защищённый программный код веб-приложений для автоматизации бизнес-процессов, реализовывать механизмы безопасной аутентификации и авторизации (OAuth 2.0, JWT), внедрять защиту от распространённых атак на уровне кода (фильтрация ввода, шифрование данных).

Владеть:

ПК-1.2/Нв1 Навыками статического и динамического анализа безопасности кода, инструментами проверки защищённости (Burp Suite, OWASP ZAP, SonarQube), методами внедрения защитных механизмов (WAF, контроль доступа, логирование) на этапе разработки и сопровождения ИС.

ПК-2 Способен к тестированию ИС и принятию мер при обнаружении инцидентов информационной безопасности, связанных с работой ИС, в рамках выполнения работ по созданию (модификации) и сопровождению ИС

ПК-2.2 Принимает меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС

Знать:

ПК-2.2/Зн1 Признаки инцидентов ИБ в веб-приложениях (OWASP Top 10: инъекции, XSS, CSRF, утечка данных, брутфорс), методы обнаружения сетевых и прикладных атак (анализ логов, WAF, IDS/IPS), процедуры реагирования на инциденты и требования к документированию в рамках сопровождения ИС.

Уметь:

ПК-2.2/Ум1 Выявлять инциденты ИБ в веб-приложениях по журналам доступа, ошибкам аутентификации и сетевым аномалиям, оперативно локализовать угрозу (блокировка IP, отключение уязвимого функционала, изоляция сегмента), применять средства защиты (WAF, антивирусы, обновление сигнатур) для купирования атак.

Владеть:

ПК-2.2/Нв1 Навыками работы с инструментами мониторинга и анализа безопасности веб-приложений (WAF, SIEM, анализаторы логов), методами сбора цифровых доказательств, приемами реагирования на инциденты, техниками документирования и составления отчётов по результатам расследования в рамках сопровождения ИС.

ПК-4 Способен к выявлению требований к Системе, ее концептуально-логическому проектированию и сопровождению разработанных проектных решений

ПК-4.1 Выявляет требования к Системе и концептуально-логически проектирует ИС

Знать:

ПК-4.1/Зн1 Методологии выявления требований к безопасности веб-приложений, классификацию угроз и уязвимостей (OWASP Top 10), принципы концептуально-логического проектирования защищённых ИС, нормативно-правовую базу защиты информации (152-ФЗ, приказы ФСТЭК), нотации моделирования (UML, BPMN, DFD) для обоснования проектных решений.

Уметь:

ПК-4.1/Ум1 Применять методы сбора и анализа требований безопасности (интервью, анализ рисков, моделирование угроз), разрабатывать концептуальные и логические модели веб-приложений с учётом требований безопасности, выявлять противоречия и риски в требованиях с использованием экспертных методов и строить диаграммы потоков данных (DFD) для обоснования проектных решений.

Владеть:

ПК-4.1/Нв1 Навыками формирования технического задания с разделом требований к безопасности веб-приложений, методами согласования требований с заинтересованными сторонами (заказчик, разработчики, эксперты ИБ), приёмами верификации и валидации проектных решений, методиками моделирования угроз и документирования результатов экспертизы.

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Безопасность Web-приложений» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 7.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

Компетенция	Предшествующие дисциплины	Последующие дисциплины
ПК-1 - Способен к разработке прототипов ИС и к созданию программного кода ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы		

ПК-1.2 Создает программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления	Безопасность мобильных приложений, Встроенные языки программирования, Методы и средства защиты информации, Организация вычислительных процессов, Основы алгоритмизации и программирования, Программно-аппаратная защита информации, Производственная практика: технологическая (проектно-технологическая) практика, Системы искусственного интеллекта, Современные технологии и языки программирования, Теория информационной безопасности и методология защиты информации, Учебная практика: ознакомительная практика, Учебная практика: технологическая (проектно-технологическая) практика, Хранение, обработка и анализ данных	Безопасность мобильных приложений, Выполнение и защита выпускной квалификационной работы, Интеллектуальные информационные системы, Программно-аппаратная защита информации, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Разработка профессиональных приложений, Современные цифровые технологии управления предприятием, Управление информационными проектами реализации комплексной безопасности
ПК-2 - Способен к тестированию ИС и принятию мер при обнаружении инцидентов информационной безопасности, связанных с работой ИС, в рамках выполнения работ по созданию (модификации) и сопровождению ИС		
ПК-2.2 Принимает меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС	Безопасность мобильных приложений, Криптографическая защита информации, Методы и средства защиты информации, Организационная защита информации, Правовая защита информации, Программно-аппаратная защита информации, Производственная практика: технологическая (проектно-технологическая) практика, Теория информационной безопасности и методология защиты информации, Техническая защита информации, Учебная практика: технологическая (проектно-технологическая) практика	Безопасность мобильных приложений, Выполнение и защита выпускной квалификационной работы, Организационная защита информации, Программно-аппаратная защита информации, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Техническая защита информации
ПК-4 - Способен к выявлению требований к Системе, ее концептуально-логическому проектированию и сопровождению разработанных проектных решений		

ПК-4.1 Выявляет требования к Системе и концептуально-логически проектирует ИС	Безопасность мобильных приложений, Встроенные языки программирования, Компьютерная экспертиза, Методы и средства защиты информации, Моделирование процессов и систем, Организационная защита информации, Организация вычислительных процессов, Основы проектной деятельности, Проектирование и реализация баз данных, Производственная практика: технологическая (проектно-технологическая) практика, Системы искусственного интеллекта, Теория информационной безопасности и методология защиты информации, Учебная практика: технологическая (проектно-технологическая) практика	Безопасность мобильных приложений, Выполнение и защита выпускной квалификационной работы, Интеллектуальные информационные системы, Компьютерная экспертиза, Организационная защита информации, Проектирование и реализация баз данных, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Современные цифровые технологии управления предприятием, Специализированные ИТ в правоохранительной деятельности, Цифровая культура в профессиональной деятельности

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Лабораторные занятия (часы)	Лекционные занятия (часы)	Индивидуальная контактная работа (часы)	Самостоятельная работа (часы)	Промежуточная аттестация
Седьмой семестр	108	3	4	2	2	0,15	85,85	Зачет
Всего	108	3	4	2	2	0,15	85,85	18

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лабораторные занятия	Лекционные занятия	Самостоятельная работа
Раздел 1. Безопасность Web-приложений	**90**	**2**	**2**	**85,85**

Тема 1.1. Введение в безопасность веб-приложений: основные понятия и определения (веб-приложение, уязвимость, атака, угроза, риск); архитектура веб-приложений (клиент-сервер, браузер, веб-сервер, БД); обзор OWASP Top 10 (инъекции, XSS, CSRF, нарушение аутентификации и др.); классификация угроз и векторов атак на веб-приложения; нормативно-правовая база защиты веб-приложений (152-ФЗ, приказы ФСТЭК).	90	2	2	85,85

5.2. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Тестовое задание
Промежуточная аттестация	Зачет

№ п/п	Наименование раздела	Вид контроля/ используемые оценочные материалы	
		Текущий	Промежут. аттестация
1	Безопасность Web-приложений	Тестовое задание	Зачет

6. Оценочные материалы текущего контроля

1. Безопасность Web-приложений Тестовое задание

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	
1	При создании программного кода веб-приложения для автоматизации бизнес-процессов, какой метод защиты от SQL-инъекций является наиболее эффективным? a) экранирование спецсимволов b) использование параметризованных запросов (prepared statements) c) удаление всех кавычек из ввода d) использование регулярных выражений		ПК-1
	Ответ:	b	
2	Какой механизм защиты должен быть реализован при создании программного кода веб-приложения для предотвращения XSS-атак? a) кодирование (экранирование) выводимых данных на стороне сервера b) использование SSL-сертификата c) отключение JavaScript в браузере d) использование CAPTCHA		ПК-1
	Ответ:	a	
3	При разработке прототипов ИС веб-приложения, какой метод аутентификации считается более безопасным для корпоративных систем? a) базовая аутентификация (Basic Auth) b) OAuth 2.0 с JWT-токенами c) аутентификация по IP-адресу d) передача пароля в открытом виде через HTTP		ПК-1
	Ответ:	b	

4	При создании программного кода веб-приложения для автоматизации бизнес-процессов, как следует хранить пароли пользователей в базе данных? a) в открытом виде b) в зашифрованном виде (AES) c) в хешированном виде с солью (bcrypt, Argon2) d) в виде MD5-хеша Ответ: c	ПК-1
5	Какой стандарт безопасности рекомендуется учитывать при разработке прототипов ИС веб-приложений для обеспечения базового уровня безопасности? a) ISO 9001 b) OWASP ASVS c) ITIL d) COBIT Ответ: b	ПК-1
6	Установите соответствие между типом уязвимости веб-приложения (1–3) и методом защиты (A–C) при создании программного кода. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). Тип уязвимости / Метод защиты в коде 1. SQL-инъекция / A. Кодирование вывода (HTML-экранирование) 2. XSS / B. Параметризованные запросы, валидация ввода 3. CSRF / C. Использование анти-CSRF токенов, проверка Referer Ответ: 1-B, 2-A, 3-C	ПК-1
7	Установите соответствие между инструментом анализа безопасности (1–3) и его назначением (A–C) при разработке прототипов ИС. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Инструмент / Назначение 1. SonarQube / A. Перехват и модификация HTTP-запросов 2. Burp Suite / B. Статический анализ кода на уязвимости 3. OWASP ZAP / C. Автоматизированное сканирование и пентест веб-приложений Ответ: 1-B, 2-A, 3-C	ПК-1
8	Установите соответствие между элементом безопасной разработки (1–3) и его описанием (A–C) при создании программного кода веб-приложений. В бланк ответов запишите последовательность (например, 1-C, 2-A, 3-B). Элемент безопасной разработки / Описание 1. Валидация ввода / A. Проверка данных на стороне клиента и сервера на соответствие ожидаемому формату 2. Кодирование вывода / B. Ограничение функционала в зависимости от роли пользователя 3. Контроль доступа (RBAC) / C. Преобразование данных перед выводом в HTML для предотвращения XSS Ответ: 1-A, 2-C, 3-B	ПК-1
9	Установите правильную последовательность этапов безопасной разработки веб-приложения при создании программного кода. Расположите буквы (A–D) в верном порядке. A) Внедрение защитных механизмов (валидация, шифрование, контроль доступа) B) Анализ требований к безопасности (моделирование угроз) C) Проведение статического и динамического анализа кода D) Разработка архитектуры с учётом безопасности Ответ: B → D → A → C	ПК-1
10	Установите правильную последовательность этапов безопасной разработки веб-приложения при создании программного кода. Расположите буквы (A–D) в верном порядке. A) Кодирование вывода (экранирование) B) Получение данных от пользователя C) Использование параметризованных запросов к БД D) Валидация данных на стороне сервера	ПК-1

	Ответ:	B → D → C → A	
11	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух методов защиты от SQL-инъекций, которые должны быть реализованы при создании программного кода веб-приложения.		ПК-1
	Ответ:	использование параметризованных запросов, валидация и фильтрация пользовательского ввода, минимальные привилегии для БД, использование ORM.	
12	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При разработке прототипов ИС веб-приложения, какой стандарт OWASP определяет требования к безопасности на уровне кода?		ПК-1
	Ответ:	OWASP ASVS (Application Security Verification Standard).	
13	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух способов защиты сессий пользователей при создании программного кода веб-приложения.		ПК-1
	Ответ:	использование Secure и HttpOnly флагов для cookie, короткое время жизни сессии, привязка сессии к IP-адресу, использование безопасных алгоритмов генерации идентификаторов.	
14	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При автоматизации бизнес-процессов в веб-приложении, какой механизм используется для безопасного хранения паролей?		ПК-1
	Ответ:	хеширование с солью (bcrypt, Argon2, PBKDF2).	
15	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух инструментов статического анализа кода, используемых при создании программного кода веб-приложений.		ПК-1
	Ответ:	SonarQube, Checkmarx, Fortify, Veracode.	
16	При обнаружении инцидента ИБ в веб-приложении, какой признак наиболее характерен для SQL-инъекции? a) ошибка в SQL-синтаксисе в ответе сервера b) замедление работы страницы c) изменение дизайна сайта d) перенаправление на другой сайт		ПК-2
	Ответ:	a	
17	При тестировании ИС для обнаружения инцидентов ИБ, какой инструмент позволяет перехватывать и модифицировать HTTP-запросы? a) Burp Suite b) Wireshark c) Nmap d) Metasploit		ПК-2
	Ответ:	a	
18	При обнаружении инцидента ИБ, связанного с XSS-атакой, какое действие должно быть выполнено в первую очередь при сопровождении ИС? a) очистка кэша сервера b) фильтрация и кодирование пользовательского ввода, обновление WAF-правил c) перезагрузка сервера d) уведомление всех пользователей		ПК-2
	Ответ:	b	
19	Какой инструмент применяется при тестировании ИС для выявления инцидентов, связанных с атаками на веб-приложения (SQLi, XSS, CSRF)? a) Wireshark b) OWASP ZAP c) Nmap d) John the Ripper		ПК-2
	Ответ:	b	
20	При принятии мер по устранению инцидента ИБ, вызванного утечкой данных, какое средство защиты должно быть применено в первую очередь? a) шифрование данных на сервере и обновление политик доступа b) отключение сервера c) удаление всех логов d) замена оборудования		ПК-2
	Ответ:	a	
21	Установите соответствие между типом инцидента ИБ (1–3) и мерой реагирования (A–C) при обнаружении инцидентов ИБ в веб-приложении. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C).		ПК-2

Инструмент	Назначение при обнаружении инцидентов ИБ
1. WAF (Web Application Firewall)	A. Перехват и анализ HTTP-трафика
2. Burp Suite	B. Фильтрация и блокировка вредоносных запросов в реальном времени

2. Burp Suite	B. Фильтрация и блокировка вредоносных запросов в реальном времени	
3. SIEM-система	C. Централизованный сбор и корреляция событий безопасности	

Ответ:	1-B, 2-A, 3-C

22	Установите соответствие между стадией реагирования на инцидент ИБ (1–3) и её содержанием (A–C) при обнаружении инцидентов ИБ и принятии мер. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). Стадия реагирования / Содержание стадии 1. Обнаружение и локализация — A. Исправление уязвимости, обновление правил WAF 2. Устранение — B. Мониторинг аномалий, идентификация затронутых компонентов 3. Анализ и предотвращение — C. Документирование, анализ причин, внедрение мер предотвращения Ответ: 1-B, 2-A, 3-C	ПК-2
23	Установите правильную последовательность действий при обнаружении инцидента ИБ в веб-приложении в рамках сопровождения ИС. Расположите буквы (A–D) в верном порядке. A) Изоляция уязвимого компонента и блокировка подозрительных IP B) Обнаружение аномалии (например, SQL-ошибка в логах) C) Устранение уязвимости (исправление кода, обновление WAF) D) Документирование инцидента и анализ причин Ответ: B → A → C → D	ПК-2
24	Установите правильную последовательность этапов тестирования ИС для обнаружения инцидентов ИБ в веб-приложении. Расположите буквы (A–D) в верном порядке. A) Перехват и анализ HTTP-запросов с помощью Burp Suite B) Запуск приложения и воспроизведение сценариев атак C) Проведение статического анализа кода (SAST) D) Проведение динамического анализа (DAST) и составление отчёта Ответ: C → B → A → D	ПК-2
25	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух признаков SQL-инъекции, которые могут быть выявлены при тестировании ИС веб-приложения. Ответ: SQL-ошибка в ответе сервера, нестандартное поведение приложения, выполнение подозрительных запросов к БД, появление данных, к которым пользователь не должен иметь доступ.	ПК-2
26	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ, связанного с XSS-атакой, какие меры должны быть приняты для защиты пользователей? Ответ: кодирование вывода, обновление правил WAF, очистка кэша пользователей, уведомление пользователей о необходимости очистки cookies.	ПК-2
27	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух инструментов, используемых при тестировании ИС для обнаружения инцидентов ИБ в веб-приложениях. Ответ: Burp Suite, OWASP ZAP, Wireshark, Nikto, Acunetix.	ПК-2
28	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ, связанного с утечкой данных, какой документ должен быть составлен в первую очередь? Ответ: акт расследования инцидента (отчёт об инциденте).	ПК-2
29	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух мер по предотвращению инцидентов ИБ в веб-приложениях. Ответ: регулярное обновление WAF-правил, проведение пентестов, обучение разработчиков безопасному кодированию, использование автоматических сканеров уязвимостей.	ПК-2
30	Установите соответствие между инструментом мониторинга (1–3) и его назначением при обнаружении инцидентов ИБ в веб-приложении (A–C). В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Инструмент / Назначение при обнаружении инцидентов ИБ 1. WAF (Web Application Firewall) — A. Перехват и анализ HTTP-трафика 2. Burp Suite — B. Фильтрация и блокировка вредоносных запросов в реальном времени 3. SIEM-система — C. Централизованный сбор и корреляция событий безопасности	ПК-2

	Ответ: 1-B, 2-A, 3-C	
31	При выявлении требований к Системе для веб-приложения, какие требования определяют необходимость использования HTTPS и шифрования данных? a) функциональные требования b) нефункциональные требования (безопасность) c) интерфейсные требования d) бизнес-ограничения Ответ: b	ПК-4
32	На этапе концептуально-логического проектирования ИС какая модель описывает потоки данных между компонентами веб-приложения и зоны доверия? a) ER-диаграмма b) DFD (диаграмма потоков данных) c) UML-диаграмма классов d) BPMN-диаграмма Ответ: b	ПК-4
33	При выявлении требований к Системе для веб-приложения, обрабатывающего персональные данные, какой нормативный документ является основным? a) ГОСТ 28147-89 b) 152-ФЗ «О персональных данных» c) ISO 9001 d) ITIL Ответ: b	ПК-4
34	Что является результатом этапа выявления требований к Системе с использованием моделирования угроз для веб-приложения? a) исходный код приложения b) модель угроз и требования к безопасности c) протоколы тестирования d) маркетинговый план Ответ: b	ПК-4
35	При концептуально-логическом проектировании ИС какая модель описывает сущности и связи для проектирования защищённой базы данных веб-приложения? a) физическая модель данных b) ER-диаграмма (сущность-связь) c) сетевая модель d) иерархическая модель Ответ: b	ПК-4
36	При выявлении требований к Системе для веб-приложения, какие требования описывают необходимость использования WAF и IDS? a) функциональные требования b) нефункциональные требования (безопасность) c) бизнес-ограничения d) интерфейсные требования Ответ: b	ПК-4
37	Установите соответствие между этапом проектирования ИС (1–3) и его содержанием (A–C) в области безопасности веб-приложений. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Этап / Содержание 1. Выявление требований — A. Построение модели угроз, выбор архитектуры защиты 2. Концептуально-логическое проектирование — B. Определение требований к аутентификации, шифрованию, WAF 3. Сопровождение проектных решений — C. Актуализация документации при изменении угроз и требований Ответ: 1-B, 2-A, 3-C	ПК-4
38	Установите соответствие между нормативным документом (1–3) и его содержанием (A–C) при выявлении требований к Системе. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). Нормативный документ / Содержание требований 1. 152-ФЗ «О персональных данных» — A. Требования к организации защиты веб-приложений	ПК-4

	2. Приказы ФСТЭК России — B. Требования к защите персональных данных в веб-приложениях 3. Постановление № 1119 — C. Уровни защищённости ИС персональных данных	
	Ответ: 1-B, 2-A, 3-C	
39	Установите соответствие между типом требования к безопасности веб-приложения (1–3) и его примером (A–C) при выявлении требований к Системе. В бланк ответов запишите последовательность (например, 1-C, 2-B, 3-A). Тип требования / Пример требования 1. Функциональное — A. «Система должна использовать WAF с обновляемыми правилами» 2. Нефункциональное (безопасность) — B. «Время восстановления после атаки не должно превышать 2 часов» 3. Нормативное — C. «Приложение должно обеспечивать двухфакторную аутентификацию» Ответ: 1-C, 2-B, 3-A	ПК-4
40	Установите правильную последовательность этапов выявления требований к безопасности для веб-приложения. Расположите буквы (A–D) в верном порядке. A) Проведение анализа рисков и идентификация угроз B) Изучение нормативно-правовых требований C) Проведение интервью с заинтересованными сторонами D) Формирование и согласование требований безопасности в ТЗ Ответ: B → C → A → D	ПК-4
41	Установите правильную последовательность этапов построения модели угроз при концептуально-логическом проектировании ИС веб-приложения. Расположите буквы (A–D) в верном порядке. A) Определение активов и их ценности B) Построение диаграммы потоков данных (DFD) C) Определение угроз и уязвимостей для каждого актива D) Разработка мер противодействия и выбор средств защиты Ответ: A → B → C → D	ПК-4
42	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух методов выявления требований к безопасности для веб-приложения. Ответ: анализ нормативных документов, проведение анализа рисков, интервьюирование заинтересованных сторон, моделирование угроз.	ПК-4
43	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Какой артефакт разрабатывается на этапе концептуально-логического проектирования ИС веб-приложения и описывает угрозы для системы? Ответ: модель угроз.	ПК-4
44	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Для чего используется диаграмма потоков данных (DFD) при концептуально-логическом проектировании веб-приложения? Ответ: для идентификации всех потоков данных, зон доверия и точек входа/выхода, что необходимо для построения модели угроз.	ПК-4
45	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух нормативных документов, требования которых должны быть выявлены при проектировании веб-приложения, обрабатывающего персональные данные. Ответ: 152-ФЗ «О персональных данных», Постановление Правительства № 1119, Приказы ФСТЭК России.	ПК-4
46	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Какой раздел технического задания должен быть обязательным при выявлении требований к Системе для веб-приложения, работающего с конфиденциальными данными? Ответ: раздел требований к информационной безопасности.	ПК-4

7. Оценочные материалы промежуточной аттестации

Зачет седьмой семестр

№ п/п	Содержание вопроса Правильный ответ (ключ ответа)	Компетенция
1	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При создании программного кода веб-приложения для автоматизации бизнес-процессов, какой метод защиты используется для предотвращения подделки межсайтовых запросов (CSRF)? Ответ: использование анти-CSRF токенов в формах и проверка заголовка Referer/Origin.	ПК-1

2	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух способов защиты от XSS-атак, которые должны быть реализованы при создании программного кода веб-приложения.		ПК-1
	Ответ:	кодирование (экранирование) вывода, валидация ввода, использование Content-Security-Policy (CSP), использование HttpOnly флага для cookie.	
3	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При разработке прототипов ИС веб-приложения, какой механизм используется для безопасного хранения сессий пользователей?		ПК-1
	Ответ:	использование серверных сессий с коротким временем жизни, хранение идентификатора сессии в HttpOnly и Secure cookie, привязка сессии к IP-адресу и User-Agent.	
4	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух инструментов, используемых при создании программного кода для статического анализа безопасности веб-приложений.		ПК-1
	Ответ:	SonarQube, Checkmarx, Fortify, Veracode, ESLint с плагинами безопасности.	
5	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При автоматизации бизнес-процессов в веб-приложении, какой механизм используется для безопасной передачи данных между клиентом и сервером?		ПК-1
	Ответ:	HTTPS (TLS/SSL) с корректно настроенными сертификатами и обязательным использованием шифрования.	
6	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ, связанного с XSS-атакой, какие меры должны быть приняты для защиты пользователей в рамках сопровождения ИС?		ПК-2
	Ответ:	кодирование вывода на всех страницах, обновление правил WAF, очистка кэша и cookies у пользователей, уведомление пользователей о необходимости смены паролей.	
7	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух признаков, указывающих на атаку типа SQL-инъекция, которые могут быть выявлены при тестировании ИС веб-приложения.		ПК-2
	Ответ:	ошибки SQL-синтаксиса в ответах сервера, выполнение подозрительных запросов к базе данных, появление несанкционированных данных, аномальное время выполнения запросов.	
8	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ, связанного с брутфорс-атакой на форму авторизации, какие меры должны быть приняты для блокировки атаки?		ПК-2
	Ответ:	блокировка IP-адреса после нескольких неудачных попыток, внедрение CAPTCHA, временная блокировка учётной записи, настройка WAF для фильтрации подозрительных запросов.	
9	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух инструментов, используемых при тестировании ИС для динамического анализа безопасности веб-приложений и обнаружения уязвимостей.		ПК-2
	Ответ:	Burp Suite, OWASP ZAP, Acunetix, Nikto, Netsparker.	
10	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При принятии мер после обнаружения инцидента ИБ, какие действия необходимо выполнить для восстановления целостности данных веб-приложения?		ПК-2
	Ответ:	восстановление данных из резервных копий, проверка целостности файлов (хеш-суммы), анализ журналов доступа для выявления изменений, удаление вредоносного кода из файлов.	
11	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При выявлении требований к Системе для веб-приложения, какие категории требований безопасности необходимо учесть для защиты от основных рисков OWASP Top 10?		ПК-4
	Ответ:	требования к аутентификации и управлению сессиями, требования к контролю доступа (RBAC), требования к валидации и санитизации ввода, требования к шифрованию данных (в покое и при передаче), требования к логированию и мониторингу, требования к защите от инъекций и XSS, требования к безопасной конфигурации сервера.	
12	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При сопровождении разработанных проектных решений веб-приложения, какие действия необходимо выполнить при изменении архитектуры системы (например, внедрение микросервисной архитектуры)?		ПК-4
	Ответ:	актуализация модели угроз (появление новых межсервисных взаимодействий), пересмотр требований к аутентификации и авторизации (OAuth 2.0, JWT, API-шлюзы), обновление схемы потоков данных (DFD) и зон доверия, внесение изменений в проектную документацию с последующим согласованием с заинтересованными сторонами.	

7.1. Уровни овладения

Компетенция: ПК-1 Способен к разработке прототипов ИС и к созданию программного кода ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы.

Индикатор достижения компетенции: ПК-1.2 Создает программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

Компетенция: ПК-2 Способен к тестированию ИС и принятию мер при обнаружении инцидентов информационной безопасности, связанных с работой ИС, в рамках выполнения работ по созданию (модификации) и сопровождению ИС.

Индикатор достижения компетенции: ПК-2.2 Принимает меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

Компетенция: ПК-4 Способен к выявлению требований к Системе, ее концептуально-логическому проектированию и сопровождению разработанных проектных решений.

Индикатор достижения компетенции: ПК-4.1 Выявляет требования к Системе и концептуально-логически проектирует ИС.

Уровень	Характеристика	Оценка в баллах

Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

8. Материально-техническое и учебно-методическое обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Щербак, А. В. Тестирование программного обеспечения: учебник для вузов / А. В. Щербак. - Москва: Юрайт, 2026. - 145 с - 978-5-534-19291-9. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/590250 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. Щербак, А. В. Информационная безопасность: учебник для вузов / А. В. Щербак. - 2-е изд. - Москва: Юрайт, 2026. - 252 с - 978-5-9916-4299-6. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/589902 (дата обращения: 21.05.2026). - Режим доступа: по подписке

Дополнительная литература

1. Козырь, Н. С. Аудит информационной безопасности: учебник для вузов / Н. С. Козырь. - Москва: Юрайт, 2026. - 36 с - 978-5-534-20647-0. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/590419 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. Козырь, Н. С. Экономические аспекты информационной безопасности: учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян. - Москва: Юрайт, 2026. - 131 с - 978-5-534-17863-0. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/589431 (дата обращения: 21.05.2026). - Режим доступа: по подписке

3. Козырь, Н. С. Оценка рисков и аудит информационной безопасности: учебник для вузов / Н. С. Козырь, В. Н. Хализев. - Москва: Юрайт, 2026. - 190 с - 978-5-534-17864-7. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/590417 (дата обращения: 21.05.2026). - Режим доступа: по подписке

8.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. https://lks.dap.gov.ru/ - Цифровая аналитическая платформа предоставления статистических данных» (ГИС ЦАП)

Ресурсы «Интернет»

1. https://stepik.org/course/207786/promo - Санкт-Петербургский политехнический университет Петра Великого — «Кибербезопасность веб-приложений» (Stepik)
Курс предназначен для начинающих специалистов в области веб-безопасности. Изучаются клиентские и серверные уязвимости, в том числе классические атаки и современные подходы к защите веб-приложений. Для успешного освоения курса рекомендуется знание основ веб-технологий и навыки программирования на Python и JavaScript.

2. https://clck.ru/3RGazU - Российское общество «Знание» — «Цифровая гигиена»
Бесплатный просветительский онлайн-курс по цифровой гигиене и безопасности в интернете. Состоит из 11 разделов с видеолекциями и конспектами, по окончании выдаётся сертификат.

3. https://fstec.ru/ - Приказы ФСТЭК России — требования к защите информации
На сайте ФСТЭК публикуются нормативные документы, регламентирующие требования к средствам защиты информации, в том числе для веб-приложений.

8.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

1. Draw.io (diagrams.net);
2. Python версии 3.14.4 ;
3. Консультант Плюс;
4. Мой офис;

Перечень информационно-справочных систем
(обновление выполняется еженедельно)

Не используется.

8.4. Специальные помещения, лаборатории и лабораторное оборудование

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения