МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.16
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность веб-приложений
(наименование дисциплины)

по направлению подготовки
09.03.03 Прикладная информатика
направленность (профиль)
Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2023

Общая трудоемкость: 4 ЗЕ

Распределение часов дисциплины по семестрам

Семестр	8	**Итого**
Форма контроля / **Вид занятий**	зачет	
Лекции	12	12
Лабораторные	16	16
Практические	32	32
Руководство: курсовые работы (проекты) / РГР[1]	-	-
Промежуточная аттестация	0,25	0, 25
Контактная работа	60,25	60,25
Самостоятельная работа	83,75	83,75
Контроль Зачет	-	-
Итого	144	144

Рабочую программу составил(и):

Додонов Алексей Владимирович

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:

☐ Отсутствует

☐ Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности) 09.03.03 Прикладная информатика

Срок действия рабочей программы дисциплины до 31.08.2027

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 2 от 05.09.2022).

1. Цель освоения дисциплины

Целью освоения дисциплины «Безопасность веб-приложений» является формирование у студентов знаний о требованиях, предъявляемых к безопасности сайта, принципах безопасной разработки сайта, типах и принципах организации атак на веб-приложения и методов, их нейтрализации. Дисциплина посвящена изучению вопросов обеспечения безопасности веб-приложений, классификации существующих уязвимостей, методам их обнаружения. Рассматриваются различные способы повышения безопасности сайтов, методы обнаружения программных закладок, безопасность программного кода, а также некоторые аспекты применения полученных знаний и умений на практике.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина:
- Основы информационной безопасности;
- Языки программирования;
- Технологии и методы программирования.

Полученные знания используются при изучении следующих дисциплин:
• Мониторинг событий информационной безопасности;
• Безопасность баз данных.

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование) [2]	**Планируемые результаты обучения**
ПК-10 Способен осуществлять моделирование решений по реализации программного обеспечения и управления БД	ПК-10.7 Использует знания основ безопасности веб приложений и веб инжиниринга	Знать: - основы безопасности веб приложений; - основы программирования; - основы веб-технологий; - протоколы передачи файлов; - классификацию веб- уязвимостей.
		Уметь: - эксплуатировать уязвимости веб приложений; - настроить SSL - сертификаты; - выбрать безопасный хостинг; - установить и настроить плагины.
		Владеть: - основами программирования; - инструментарием QSINT.
	ПК-10.8 Умеет организовать аудит программного кода веб приложения, применять инструменты для поиска уязвимостей	Знать: - средства и инструменты анализа защищенности сайта
		Уметь: - организовать аудит программного кода веб приложения

[2] Для программ по ФГОС 3, 3+ – индикаторы достижения компетенций не указываются, ставится прочерк «–», указываются только компетенции и планируемые результаты обучения.

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование) [2]	**Планируемые результаты обучения**
		Владеть: - навыками установки и настройки безопасных механизмов
	ПК-10.9 Владеет методами обнаружения атак на веб - приложения	Знать: - методику и проведение анализа защищенности сайта
		Уметь: - применять инструменты для поиска уязвимостей
		Владеть: - методами обнаружения атак на веб - приложения

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1	Лек	Тема 1 Основы безопасности веб-приложений. Основные принципы построения безопасных сайтов. Понятие безопасности приложений и классификация опасностей. Источники угроз информационной безопасности сайтов. База данных общеизвестных уязвимостей. Безопасная аутентификация и авторизация Структура сайта, ПО веб сервера Введение в разведку веб-приложений. Структура современных веб-приложений. Принципы и среда разработки кода приложений. Понятие хостинга, сертификатов, плагинов. Особенности протоколов http и https. Сбор информации о web-приложении.	8	2		-	
Модуль 1	Пр	Тема 1 Основы безопасности веб-приложений. Оценка стойкости пароля на основе энтропии и словарей	8	2			Отчёт по практической работе № 1
Модуль 1	Ср	Тема 1 Основы безопасности веб-приложений.	8	14			
Модуль 1	Лаб	Тема 1 Структура сайта, ПО веб сервера Лабораторная работа Пассивный сбор информации о web-приложении	8	2			
Модуль 1	Пр	Тема 1 Структура сайта, ПО веб сервера Размещение сайта на хостинге	8	2			Отчёт по практической работе № 2
Модуль 1	Пр	Тема 1 Структура сайта, ПО веб сервера Установка сертификатов, создание самоподписанных сертификатов	8	2			Отчёт по практической работе № 3
Модуль 1	Лек	Тема 2 Технологии взлома сайта	8	2			

		Принципы этичного хакинга. Поиск слабых мест в архитектуре приложения. Поиск субдоменов. Анализ API. Обнаружение сторонних зависимостей. Методы, основанные на использовании тега <IFRAME>.					
Модуль 1	Пр	Тема 2 Технологии взлома сайта Выявление векторов атаки на web-приложение	8	2			Отчёт по практической работе № 4
Модуль 1	Пр	Тема 2 Технологии взлома сайта Поиск уязвимых зависимостей и плагинов web-приложения	8	2			Отчёт по практической работе № 5
Модуль 1	Ср	Тема 2 Технологии взлома сайта	8	14			
Модуль 1	Лек	Тема 3 Виды атак на веб серверы Активный фаззинг веб-приложения. Атаки методом грубой силы. Понятие LDAP (Lightweight Directory Access Protocol), методы атак на LDAP. SQL-инъекция. XSS-атаки. Атаки PHP injection. Атака на внешние сущности XML (XXE). CMD injection и удаленное выполнение кода на сервере. Отказ в обслуживании. Прикладные техники разведки и нападения	8	2			
Модуль 1	Лаб	Тема 3 Виды атак на веб серверы Активный сбор информации о веб-приложении	8	2			
Модуль 1	Пр	Тема 3 Виды атак на веб серверы Атаки методом грубой силы	8	2			Отчёт по практической работе № 6
Модуль 1	Пр	Тема 3 Виды атак на веб серверы Настройка авторизации через LDAP	8	2			Отчёт по практической работе № 7
Модуль 1	Пр	Тема 3 Виды атак на веб серверы Практическое применение Union-based SQL injection	8	2			Отчёт по практической работе № 8
Модуль 1	Пр	Тема 3 Виды атак на веб серверы Практическое применение Blind-based SQL injection	8	2			Отчёт по практической работе № 9

Модуль 1	Пр	Тема 3 Виды атак на веб серверы Автоматизация SQL-инъекций. Работа с sqlmap	8	2			Отчёт по практической работе № 10
Модуль 1	Пр	Тема 3 Виды атак на веб серверы Эксплуатация XSS-атак.	8	2			Отчёт по практической работе № 11
Модуль 1	Пр	Тема 3 Виды атак на веб серверы Внедрение файлов через PHP-инъекции	8	2			Отчёт по практической работе № 12
Модуль 1	Пр	Тема 3 Виды атак на веб серверы Возможности RCE для повышения привилегий	8	2			Отчёт по практической работе № 13
Модуль 1	Ср	Тема 3 Виды атак на веб серверы	8	14			
Модуль 1	Лек	Тема 4 Обнаружение атак, уязвимостей сайтов и приложений Тестирование на устойчивость к атакам. Методы обнаружения вредоносных программ. Обзор и применение ПО для сканирования уязвимостей приложений. Подделка параметров запроса. Обнаружение RCE (Remote Code Execution). Программы Bug Bounty. Динамический и статический анализ. Выявление эскалации привилегий	8	2			
Модуль 1	Лаб	Тема 4 Обнаружение атак, уязвимостей сайтов и приложений Тестирование на устойчивость к атакам отказа в обслуживании	8	2			
Модуль 1	Пр	Тема 4 Обнаружение атак, уязвимостей сайтов и приложений Обнаружение атак в реальном времени	8	2			Отчёт по практической работе № 14
Модуль 1	Пр	Тема 4 Обнаружение атак, уязвимостей сайтов и приложений Инструменты защиты веб-приложений	8	2			Отчёт по практической работе № 15

Модуль 1	Лаб	Тема 4 Обнаружение атак, уязвимостей сайтов и приложений Лабораторная работа Применение сканеров по анализу защищенности сайтов	8	2			
Модуль 1	Ср	Тема 4 Обнаружение атак, уязвимостей сайтов и приложений	8	14			
Модуль 1	Лек	Тема 5 Защита веб приложений от атак. Средства защиты. Общая отказоустойчивость системы. Меры по защите от интернет-атак. Защита от исполнения вредоносного кода в браузере. Проверка безопасности кода. Использование возможностей антивирусного ПО для защиты веб-приложений. Обзор, настройка, использование WAF. Защита критичных данных.	8	2			
Модуль 1	Лаб	Тема 5 Защита веб приложений от атак. Средства защиты. Защита веб-приложения от атак SQL injection	8	2			
Модуль 1	Лаб	Тема 5 Защита веб приложений от атак. Средства защиты. Настройка прав доступа для ограничения RCE	8	2			
Модуль 1	Лаб	Тема 5 Защита веб приложений от атак. Средства защиты. Защита веб-приложения от атак XSS	8	2			
Модуль 1	Лаб	Тема 5 Защита веб приложений от атак. Средства защиты. Настройка WAF	8	2			
Модуль 1	Ср	Тема 5 Защита веб приложений от атак. Средства защиты.	8	14			

Модуль 1	Лек	Тема 6 Регламенты и методы разработки безопасных веб-приложений Выбор безопасного хостинга. Установка и настройка механизмов безопасности сайта (перенаправление на HTTPS, скрытие панелей управления, настройка прав доступа, включение автоматического обновления и т.п.). Выбор и установка SSL-сертификата для сайта. Установка и безопасности настройки плагинов. Включение механизмов защиты (регламентация смены паролей привилегированных пользователей, многофакторная аутентификация, настройка DKIM и SPF для почты.). Антипаттерны безопасного программирования. Приемы написания кода для противодействия XSS. Противодействие внедрению SQL-кода. Функции контроля доступа.	8	2			
Модуль 1	Пр	Тема 6 Регламенты и методы разработки безопасных веб-приложений Пр. 16. Техники безопасной разработки	8	2			Отчёт по практической работе № 16
	Ср	Тема 6 Регламенты и методы разработки безопасных веб-приложений	8	13,75			
	ПА	Сдача зачёта	8	0.25			Вопросы к зачёту
			Итого	144			

5. Образовательные технологии

Лекции и практические занятия с использованием презентаций и демонстрационных примеров, экзамен. Для получения обратной связи от студентов и повышения уровня заинтересованности студента в предмете, используются такие активные и интерактивные формы обучения как: лекции-беседы, лекции и практики с запланированными ошибками. В течение семестра студенты решают задачи, указанные преподавателем. Для выполнения практических работ разработаны задания. Так же разработан лекционный курс. Допуск к экзамену осуществляется при выполнении всех практических заданий.

6. Методические указания по освоению дисциплины

6.1. Рекомендации по освоению лекционного материала, подготовке к лекциям

Лекции являются одним из основных видов учебных занятий в высшем учебном заведении. В ходе лекционного курса проводится изложение современных научных материалов в систематизированном виде, а также разъяснение наиболее трудных вопросов учебной дисциплины. При изучении дисциплины следует помнить, что лекционные занятия являются направляющими в большом объеме научного материала. Большую часть знаний студент должен набирать самостоятельно из учебников и научной литературы. Конспекты лекций рекомендуется использовать при подготовке к лабораторным занятиям, экзамену, контрольным тестам, при выполнении самостоятельных заданий.

. 6.2. Рекомендации по организации самостоятельной работы

Для выполнения самостоятельной работы студентам предлагается ряд интернет ресурсов по безопасности web-приложений. Текущий контроль успеваемости осуществляется на основе контроля выполнения заданий, выданных на практических занятиях.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр[3]	**Код контролируемой компетенции (или ее части)**	**Наименование оценочного средства**[4]
8	ОПК-10	Вопросы к зачёту № 1-45
		Отчёты по практическим работам № 1-16

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1. Выполнение практических заданий

Темы практических работ

№ п/п	**Темы**
1	Оценка стойкости пароля на основе энтропии и словарей
2	Размещение сайта на хостинге
3	Установка сертификатов, создание самоподписанных сертификатов
4	Выявление векторов атаки на web-приложение
5	Поиск уязвимых зависимостей и плагинов web-приложения

[3] Если дисциплина реализуется несколько семестров, то семестры указываются в одной таблице по порядку.

[4]Указываются оценочные средства для каждой компетенции в соответствии с Разделом 4 (примечание: не каждую компетенцию можно проверить вопросом к зачету/экзамену, т.е. не по каждой компетенции могут быть указаны вопросы к зачету/экзамену; однако все вопросы к зачету/экзамену в совокупности должны быть указаны в графе «Наименование оценочного средства»).

№ п/п	Темы
6	Атаки методом грубой силы
7	Настройка авторизации через LDAP
8	Union-based SQL injection
9	Blind-based SQL injection
10	Автоматизация SQL-инъекций. Работа с sqlmap
11	Эксплуатация XSS-атак.
12	Внедрение файлов через PHP-инъекции
13	Возможности RCE для повышения привилегий
14	Обнаружение атак в реальном времени
15	Инструменты защиты веб-приложений
16	Техники безопасной разработки

Типовой(ые) пример(ы) задания(ий)

При выполнении практических заданий студенты устанавливают сертификаты, изучают вектора атак и способы обнаружения и защиты, типы веб атак, применяют теоретические знания для практических навыков по обнаружению и эксплуатации уязвимостей, сканированию веб приложений, знакомятся с техникой безопасной разработки веб приложений.

Краткое описание и регламент выполнения

1. Изучить теоретический материал и нормативно-правовую базу.
2. Оформить отчет о практической работе в соответствии с требованиями к оформлению практических работ в соответствии с тематикой задания.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если практическое задание выполнено грамотно или имеет несущественные замечания, выполнен отчет по работе.

- оценка «не зачтено» выставляется студенту, если практическое задание не выполнено, имеет грубые ошибки, не подготовлен отчет.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 8

№ п/п	Вопросы к зачету
1	Атака «злоупотребление функциональностью». Привести примеры. Дать рекомендации по минимизации рисков возникновения данного типа атаки.
2	Атака с внедрением SQL инъекции. Привести примеры. Методы защиты от union-based инъекций.
3	Атака «межсайтовый скриптинг». Привести примеры. Способы защиты
4	Атака CRSF: методы и утилиты. Меры, применяемые для минимизации успешности данного типа атаки.
5	Атака «переполнение буфера». Причина возникновения, примеры.
6	Атака «отказ в обслуживании». Классификация методов. Меры, применяемые для минимизации успешности данного типа атак.
7	Поиск WEB уязвимостей
8	Системы и ПО для обнаружения атак
9	Методы распространения вредоносного программного кода
10	Источники угроз информационной безопасности сайтов
11	Структура современных веб-приложений
12	Методы поиска субдоменов
13	Понятие LDAP. Использование в качестве инструмента авторизации.
14	Особенности атак с использованием протокола Kerberos
15	Прикладные техники разведки и нападения
16	Методы обнаружения вредоносных программ
17	Условия и примеры программ Bug Bounty
18	Методика проверки безопасности кода
19	Платформы разработки веб приложений
20	Настройка и использование централизованного антивирусного ПО
21	Как производится выбор и установка SSL-сертификата
22	Что такое WAF, обзор продуктов, использование
23	Установка и безопасность настройки плагинов
24	Обзор сканеров для поиска уязвимостей веб приложений, сайтов
25	Общие требования к безопасности сайтов
26	Настройка панели администратора сайта с целью минимизации ущерба при взломе
27	Примеры мер защиты от внедрения вредоносного кода
28	Этапы проведения атаки на веб приложение
29	Этапы проверки безопасности сайта
30	Выявление эскалации привилегий и способы её предотвращения
31	Подделка параметров запросов. Использование cookies в запросах
32	Поиск уязвимостей SQL injection через sqlmap. Преимущества и недостатки относительно ручного поиска
33	Активный фаззинг веб-приложения
34	Способы защиты веб-приложения от атак методом грубой силы
35	Атаки PHP injection. Примеры, способы защиты

№ п/п	Вопросы к зачету
36	Методы аутентификации в приложении. Способы двухфакторной аутентификации
37	Банк данных угроз безопасности информации ФСТЭК России. Запись уязвимостей, практическое применение
38	Common Vulnerabilities and Exposures. Запись уязвимостей, практическое применение
39	Реагирование на атаки в реальном времени. Привести примеры для атак типа «отказ в обслуживании», для случаев эскалации привилегий, для удалённого выполнения кода.
40	Принципы этичного хакинга. Последствия их нарушений
41	Контроль доступа к веб-приложению. Ограничения прав системных учётных записей, привести практические примеры.
42	Принципы безопасной разработки API
43	Выбор безопасного хостинга. Принципы создания бэкапов сайта
44	Организационные меры безопасности для защиты веб-приложений
45	Определение критичности данных, особенности защиты критичной информации

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
8	Зачет	«зачтено»	55-100 баллов
		«не зачтено»	0-54 баллов

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС[5]
1	Э. Хофман	Безопасность веб-приложений	учебно-методическое пособие	СПб.: Питер, 2021	
2	СТРК	Разработка безопасного программного обеспечения	ГОСТ Р 56939-2016	2021 г.	
3	П. Яворски	Полевое руководство по веб хакингу		СПб.: Питер, 2020	

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1		The Web Application Security Consortium. The WASC Threat Classification v2.0			Электон. текстовые дан. — Режим доступа: http://projects.webappsec.org/w/page/13246978/Threat Classification,

8.3. Перечень профессиональных баз данных и информационных справочных систем[6]

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	OfficeStandart	OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3.	Консультант+	Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
2	"Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. УЛК -310	Столы ученические., стол преподавательский, стулья, доска (маркерная), кафедра напольная, ПК , телевизор.

[6] *Базы данных и информационные справочные системы должны быть актуальны.*

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
3	Помещение для самостоятельной работы обучающихся Г-401	Столы, стулья, компьютеры
4	Помещение для самостоятельной работы обучающихся Д -409	Столы-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф