Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет имени В.А. Бондаренко»

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.22 Безопасность веб-приложений»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
10.03.01 Информационная безопасность
(код и наименование направления подготовки)

Безопасность автоматизированных систем (информационные технологии и электронная промышленность)
(наименование направленности (профиля) образовательной программы)

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2026

Рабочая программа дисциплины «*Б1.Д.Б.22 Безопасность веб-приложений*» рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 10 от "06" 03 20 26 г.

Заведующий кафедрой
Кафедра вычислительной техники и защиты информации В.В. Тугов
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
Доцент кафедры ВТиЗИ А.А. Рычкова
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
10.03.01 Информационная безопасность В.В. Тугов
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
главный библиограф Г.С. Гаваитис
личная подпись *расшифровка подписи*

Уполномоченный по качеству института
С.Н. Морозова
личная подпись *расшифровка подписи*

№ регистрации _____

© Рычкова А.А., 2026
© ОГУ, 2026

1 Цели и задачи освоения дисциплины

Цель: формирование у обучающихся теоретических знаний и практических навыков по выявлению, анализу и устранению уязвимостей веб-приложений, а также развитие способности документировать результаты аудита безопасности и вести профессиональную коммуникацию по вопросам защиты информации.

Задачи:

1. Изучить архитектуру веб-приложений и типовые модели угроз.
2. Освоить методологии тестирования на проникновение (OWASP).
3. Научиться применять нормативные правовые акты в области защиты информации при анализе защищенности веб-систем.
4. Сформировать навыки составления экспертных заключений и отчетов по результатам аудита.
5. Развить умение аргументированно обсуждать меры защиты с заказчиком на русском и профессиональном английском языке.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.11 Русский язык и культура речи, Б1.Д.Б.23 Информатика*

Постреквизиты дисциплины: *Б1.Д.Б.34 Проектирование систем информационной безопасности*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
УК-4 Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	УК-4-В-1 Выбирает на государственном и иностранном (-ых) языках коммуникативно приемлемый стиль делового общения, вербальные и невербальные средства взаимодействия с партнерами УК-4-В-2 Ведет деловую коммуникацию в письменной и электронной форме, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках	**Знать:** Нормы официально-делового и научного стилей русского языка; правила использования профессиональной терминологии по веб-безопасности на русском и английском языках; особенности невербальных средств в переговорах по ИБ. Структуру официальных писем (запрос на проведение аудита, акцепт), особенности англоязычной корреспонденции в ИБ-сфере; правила

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		оформления технической документации (ГОСТы). **Уметь:** Выбирать коммуникативно приемлемый стиль при обсуждении уязвимостей с разработчиками (неофициально) и с руководством (официально); использовать англоязычные термины (XSS, SQLi, CSRF) в речи. Вести переписку с владельцами веб-ресурсов; составлять отчет о тестировании на проникновение (письменная форма) с учетом стилистики официального документа; переводить профильную терминологию. **Владеть:** Навыками переключения стилей общения в зависимости от аудитории (технические специалисты / менеджмент); навыками устного доклада на русском и английском по результатам пентеста. Навыками составления актов, протоколов согласования, executive summary отчета; навыками письменной аргументации мер защиты на двух языках.
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5-В-1 Использует нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере информационных технологий и телекоммуникаций	**Знать:** Ключевые нормативно-правовые акты РФ в сфере ИБ: Приказы ФСТЭКК; стандарты OWASP, ГОСТ 56545-2015 **Уметь:** Применять нормативные требования к защите веб-приложений (уровень

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		защищенности ПДн); соотносить найденную уязвимость с пунктами методических документов; обосновывать необходимость средств защиты. **Владеть:** Методикой выбора контрмер на основе базы требований НПА; навыками составления заявок на сертификацию (при наличии веб-портала).
ОПК-4.1 Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1-В-1 Организует и проводит аудит, модернизацию, разработку и внедрение систем защиты информации	**Знать:** Методики аудита защищенности веб-приложений (статический анализ кода, динамическое тестирование, пентест); этапы внедрения Web Application Firewall (WAF); порядок модернизации систем защиты **Уметь:** Планировать и проводить организационные мероприятия: сбор данных, согласование графика аудита; разрабатывать технические задания на модернизацию СЗИ; внедрять политики безопасной разработки (SDLC). **Владеть:** Навыками организации команды для «красной команды»; навыками составления плана внедрения средств защиты (WAF, RASP) и оценки их эффективности.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	3 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**52,25**	**52,25**
Лекции (Л)	18	18
Лабораторные работы (ЛР)	34	34
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение индивидуального творческого задания (ИТЗ);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- изучение разделов курса в системе электронного обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к рубежному контролю)*	**55,75**	**55,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**диф. зач.**	

Разделы дисциплины, изучаемые в 3 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Основы безопасности веб-приложений	16	2		4	10
2	Нормативно-правовое регулирование и документация	20	4		6	10
3	Технические уязвимости веб-приложений	34	4		18	12
4	Аудит безопасности и инструментарий	22	4		6	12
5	Организация мероприятий по защите и отчетность	16	4			12
	Итого:	108	18		34	56
	Всего:	108	18		34	56

4.2 Содержание разделов дисциплины

Раздел 1. Основы безопасности веб-приложений

Архитектура клиент-сервер. Модель OSI и прикладной уровень. Протокол HTTP/HTTPS (методы, заголовки, cookies, сессии). Классификация угроз OWASP Top 10 (актуальная версия). Понятие модели угроз и модели нарушителя для веб-систем.

Раздел 2. Нормативно-правовое регулирование и документация

Составление технического задания на аудит защиты веб-приложения. Организационно-распорядительная документация (приказы, акты допуска). Англоязычная терминология в контрактах на пентест.

Раздел 3. Технические уязвимости веб-приложений

SQL-инъекции. Техники эксплуатации и защита (параметризация запросов). Аутентификация (атаки на сессии, брутфорс, восстановление паролей). Утечка конфиденциальных данных (TLS, анализ шифрования). Нарушение контроля доступа (подмена параметров, вертикальное/горизонтальное повышение привилегий). Межсайтовый скриптинг (XSS).

Раздел 4 Аудит безопасности и инструментарий

Статический (SAST) и динамический (DAST) анализ. Инструменты. Применение брандмауэра веб-приложений (WAF). Управление уязвимостями (CVSS, базы CVE).

Раздел 5 Организация мероприятий по защите и отчетность

Жизненный цикл безопасной разработки (SDLC). Роли в команде разработки и ИБ (DevSecOps). Составление отчета о пентесте.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Создание веб-приложения	4
1	2	Анализ архитектуры и модели угроз веб-приложения: OSINT	6
2	3	Инъекции кода (SQL): эксплуатация, документация и нормативное обоснование	6
3	3	Нарушение контроля доступа: сценарии атак на бизнес-логику	6
4	3	Межсайтовый скриптинг XSS и защита от него	6
5	4	Аудит безопасности с использованием WAF и сканера уязвимостей	6
		Итого:	34

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Дунаев, В. В. Web-программирование для всех [Текст] / В. В. Дунаев. - СПб. : БВХПетербург, 2008. - 560 с. : ил. - Прил.: с. 505-546. - Библиогр.: с. 547. - Предм. указ.: с. 548-550. - ISBN 978-5-9775-0197-2/

2. Шаньгин, В. Ф.Информационная безопасность компьютерных систем и сетей [Текст] : учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей "Информатика и вычислительная техника" / В. Ф. Шаньгин. - Москва : Форум : ИНФРА-М, 2014. - 416 с. : ил. - Библиогр.: с. 401-408. - ISBN 978-5-8199-0331-5. - ISBN 978-5-16-003132-3.

5.2 Дополнительная литература

1. Позевалкин, В. В.Теория и практика разработки интернет-приложений [Электронный ресурс] : учебное пособие для обучающихся по образовательной программе высшего образования по направлению подготовки 09.03.03 Прикладная информатика / В. В. Позевалкин, Н. Ф. Панова; М-во науки и высш. образования Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования "Оренбург. гос. ун-т". - Электрон. текстовые дан. (1 файл: 3.72 Мб). - Оренбург : ОГУ, 2023. - 223 с. - Загл. с тит. экрана. - Adobe Acrobat Reader 8.0. - Режим доступа: http://artlib.osu.ru/web/books/metod_all/196831_20231201.pdf - ISBN 978-5-7410-3153-7.

2. Тишина, Н. А. Прикладные задачи безопасности информационно-телекоммуникационных систем [Электронный ресурс] : учебное пособие для обучающихся по образовательной программе высшего образования по направлению подготовки 09.04.04 Программная инженерия / Н. А. Тишина, Е. Н. Чернопрудова; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват.

учреждение высш. образования "Оренбург. гос. ун-т", Каф. прогр. обеспечения вычисл. техники и автоматизир. систем. - Электрон. текстовые дан. (1 файл: 2.22 Мб). - Оренбург : ОГУ, 2017. - 121 с. - Загл. с тит. экрана. - Adobe Acrobat Reader 6.0. - Режим доступа: http://artlib.osu.ru/web/books/metod_all/60117_20171205.pdf - ISBN 978-5-7410-1892-7.

5.3 Периодические издания

1. Автоматизация в промышленности: журнал. - М.:Изд. дом "Инфоавтоматизация", 2026.
2. Программирование: журнал. – М.: Изд. «Национальная платформа научных периодических изданий», 2026.
3. Информационные технологии в проектировании и производстве: журнал. – М.: Изд. «ФГУП НТЦ оборонного комплекса «Компас», 2026.

5.4 Интернет-ресурсы

1 http://www.rsl.ru/ - Российская государственная библиотека.
2 http://window.edu.ru/ - ИС «Единое окно доступа к образовательным ресурсам.
3 http://e.lanbook.com/– Электронная библиотечная система «Издательство «Лань».
4 http://www.biblio-online.ru – Электронная библиотека издательства «Юрайт».
5 http://www.iprbookshop.ru - Электронная библиотечная система IPRbooks.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.

2. Пакет офисных приложений «МойОфис Образование»

3. Для работы с ресурсами Интернет - веб-браузер Яндекс https://yandex.ru/..

4. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2026]. – Режим доступа в сети ОГУ http://garant.net.osu.ru

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется компьютерный класс, оснащенный плакатами.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.