Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.44.3 Уязвимость программного обеспечения»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2025

2207364

Рабочая программа дисциплины «*Б1.Д.Б.44.3 Уязвимость программного обеспечения*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 7 от "21" февраля 2025 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем — И.В. Влацкая
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
Доцент — Ю.Д. Фот
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность — И.В. Влацкая
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
Н.Н. Бигалиева
личная подпись *расшифровка подписи*

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

№ регистрации _____

© Фот Ю.Д., 2025
© ОГУ, 2025

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

Развитие у будущих специалистов навыков по выявлению уязвимых мест в программном обеспечении, угроз, направленных на их эксплуатацию, а также навыков по разработке необходимых средств защиты.

Задачи:

- изучение типовых классификаций угроз безопасности, уязвимых мест в программном обеспечении, атак, систем оценивания степени риска;
- изучение основных угроз, уязвимых мест и средств защиты Web-приложений;
- получение навыков разработки программ для X509 и подписания сборок и приложений;
- изучение принципов работы многофакторной аутентификации, механизмов генерации одноразовых паролей.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.34 Защита программ и данных, Б1.Д.Б.37 Техническая защита информации, Б1.Д.Б.44.2 Анализ программных реализаций*

Постреквизиты дисциплины: *Б2.П.В.П.1 Производственная практика (по специализации), Б2.П.В.П.2 Преддипломная практика*

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
ОПК-3.1 Способен проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей	ОПК-3.1-В-1 Знает основные типовые классификации угроз безопасности, уязвимых мест в программном обеспечении, атак, систем оценивания степени риска; основные угрозы, уязвимые места и средства защиты Web-приложений ОПК-3.1-В-2 Способен выявлять различного рода уязвимости в разрабатываемом программном обеспечении, включая возможности для SQL-инъекции, XSS- и CSRF-атак ОПК-3.1-В-3 Владеет первичными навыками проведения экспериментально-исследовательских работ при проведении сертификации средств защиты информации ОПК-3.1-В-4 Владеет навыками использования	**Знать:** - основные типовые классификации угроз безопасности, уязвимых мест в программном обеспечении, атак, систем оценивания степени риска; - основные угрозы, уязвимые места и средства защиты Web-приложений. **Уметь:** - выявлять различного рода уязвимости в разрабатываемом программном обеспечении, включая возможности для SQL-инъекции. **Владеть:** - первичными навыками проведения экспериментально-исследовательских работ при проведении сертификации средств защиты информации. - навыками использования инструментальных средств отладки и дизассемблирования программного

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	инструментальных средств отладки и дизассемблирования программного кода	кода.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 академических часа).

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**61,25**	**61,25**
Лекции (Л)	30	30
Лабораторные работы (ЛР)	30	30
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- написание реферата (Р);* *- изучение разделов курса «Уязвимость программного обеспечения» в системе электронного обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к рубежному контролю.*	**82,75**	**82,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в предмет	40	10		6	24
2	Уязвимости Web-приложений	56	10		16	30
3	Тестирование на проникновение и сканирование	48	10		8	30
	Итого:	144	30		30	84
	Всего:	144	30		30	84

4.2 Содержание разделов дисциплины

1 Введение в предмет. Основные понятия информационной безопасности: уязвимость, угроза, атака, злоумышленник, эксплоит. Классификация угроз информационной безопасности, классификация атак. Подходы к обеспечению безопасности информационной системы. Уязвимости информационных систем. Правила описания уязвимостей.

2 Уязвимости Web-приложений. Тестирование защищенности транспортного уровня. Тестирование защищенности механизма управления доступом. Тестирование защищенности механизма управления сессиями. Тестирование на устойчивость к атакам отказа в обслуживании. Поиск уязви-

мостей к атакам CSRF. Поиск уязвимостей к атакам XSS. Поиск уязвимостей к атакам SQL-injection. Поиск уязвимостей к атакам RCE. Сканирование уязвимостей веб-приложений.

3 Тестирование на проникновение и сканирование. Теоретические основы тестирования на проникновение. Получение информации от DNS-сервера. Поиск и эксплуатации уязвимостей. Парольные атаки на различные сервисы. Средство для тестирования эксплойтов. Нагрузочное тестирование. DDoS (Distributed Denial of Service) - основные особенности их организации и защиты от них.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Основы анализа уязвимостей. Системы классификации и оценки уязвимостей	2
2	1	SonarQube. Инструмент статического анализа кода	2
3	1	Использование инструментов динамического анализа. Burp Suite	2
4	2	Настройка и использование сканера уязвимостей OpenVAS	2
5	2	Оценка уязвимостей веб-приложений с помощью Wfuzz	2
6	2	Система мониторинга Prometheus	2
7	2	SQL-уязвимости и защита от них	2
8	2	Обнаружение XSS-уязвимостей и борьба с ними	2
9	2	Metasploit	2
10	2	SkipFish. Инструмент поиска уязвимостей WEB-приложений	2
11	2	OWASP. Тестирование Web-приложений	2
12	3	Тестирование на проникновение. Legion	2
13	3	JMeter для нагрузочного тестирования и тестирования производительности	2
14,15	3	DDoS-атаки – основные особенности их организации	4
		Итого:	30

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Алѐшкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алѐшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167600 (дата обращения: 28.02.2025). — Режим доступа: для авториз. пользователей.

2. Никитин, В. Н. Проведение анализа защищённости информации в информационной системе : учебное пособие / В. Н. Никитин. — Хабаровск : ДВГУПС, 2020. — 79 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/179382 (дата обращения: 28.02.2025). — Режим доступа: для авториз. пользователей.

5.2 Дополнительная литература

1. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах [Текст] : учеб. пособие / П. Б. Хорев.- 4-е изд., стер. - М. : Академия, 2008. - 256 с. : ил. - (Высшее профессиональное образование). - Библиогр.: с. 251-252. - ISBN 978-5-7695-5118-5.

2. Теоретические основы компьютерной безопасности [Текст] : учеб. пособие для вузов / П. Н. Девянин [и др.]. - М. : Радио и связь, 2000. - 192 с. : ил. - Авт. указаны на обороте тит. л.. - Библиогр. в конце гл. - ISBN 5-256-01413-7.

3. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 28.02.2025). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

4. Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва : РТУ МИРЭА, 2020. — 136 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167606 (дата обращения: 28.02.2025). — Режим доступа: для авториз. пользователей.

5.3 Периодические издания

1. Информация и безопасность : журнал. - М. : Агентство "Роспечать".
2. Вестник информационной безопасности : журнал. - М. : Агенство "Роспечать".
3. Системы безопасности : журнал. - М. : Агентство "Роспечать".
4. Проблемы информационной безопасности. Компьютерные системы : журнал. - М. : АПР.

5.4 Интернет-ресурсы

1. SQL injection для начинающих. Часть 1. – Режим доступа: https://habrahabr.ru/post/148151/
2. OWASP. the free and open software security community. – Режим доступа: https://www.owasp.org/index.php/Main_Page
3. Strong-Named Assemblies. – Режим доступа: https://docs.microsoft.com/en-us/dotnet/framework/app-domains/strong-named-assemblies

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

а) программно-аппаратное обеспечение:

1. Операционная система Astra Linux. «Astra Linux Special Edition» РУСБ.10015-01, лицензионный договор №А-2021-1374-ВУЗ от 28.05.2021
2. Open Office/LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Metasploit Framework. Доступна бесплатно. Режим доступа:https://www.metasploit.com/
4. Nmap. Доступна бесплатно. Режим доступа:https://nmap.org/
5. Cuckoo Sandbox. Доступна бесплатно. Режим доступа: https://cuckoosandbox.org/
6. Snort. Доступна бесплатно. Режим доступа: https://snort.ru.uptodown.com/windows
7. Karkinos. Доступна бесплатно. Режим доступа: https://github.com/helich0pper/Karkinos
8. Sifter. Доступна бесплатно. Режим доступа: https://github.com/s1l3nt78/sifter
9. Sn1per. Доступна бесплатно. Режим доступа: https://github.com/1N3/Sn1per
10. Commix. Доступна бесплатно. Режим доступа: https://commixproject.com/
11. Browser Exploitation Framework (BeEF) Доступна бесплатно. Режим доступа: https://beefproject.com/

б) базы данных, информационно-справочные и поисковые системы:

– Консультант Плюс [Электронный ресурс] : справочно-правовая система / Компания Консультант Плюс. – Электрон. дан. – Москва, [1992–2016]. – Режим доступа : в локальной сети ОГУ \\fileserver1\!CONSULT\cons.exe

– Гарант [Электронный ресурс] : справочно-правовая система / НПП Гарант-Сервис. – Электрон. дан. - Москва, [1990–2016]. – Режим доступа \\fileserver1\GarantClient\garant.exe. В локальной сети ОГУ.

– Законодательство России [Электронный ресурс] : информационно-правовая система. – Режим доступа : http://pravo.fso.gov.ru/ips/, в локальной сети ОГУ.

– Открытые поисковые системы
– OWASP https://owasp.org/www-project-top-ten//
– CVE https://cve.mitre.org//
– Common Attack Pattern Enumeration and Classification (CAPEC) https://capec.mitre.org/.
– Банк данных угроз безопасности информации https://bdu.fstec.ru/vul.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, курсового проектирования, 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 персональными компьютерами с установленным программным обеспечением.

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

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.