Минобрнауки России

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

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«С.1.Б.41.3 Уязвимость программного обеспечения»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность

10.05.01 Компьютерная безопасность
(код и наименование специальности)

Разработка защищенного программного обеспечения
(наименование направленности (профиля) образовательной программы)

Квалификация

Специалист по защите информации

Форма обучения

Очная

Год набора 2018

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № _____ от "___" _____ 20__ г.

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

Исполнители:
Старший преподаватель К. К. Шпинёв
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 комплектования научной библиотеки
личная подпись Н.Н. Грицай *расшифровка подписи*

Уполномоченный по качеству факультета
личная подпись И.В. Крючкова *расшифровка подписи*

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

Формирование теоретических знаний и практических навыков по выявлению уязвимых мест в программном обеспечени. Изучение технологий выявления уязвимостей, угроз, направленных на их эксплуатацию. Формирование знаний и навыков по разработке средств защиты. Путем внедрения уязвимостей в тестовое приложение обучить на практике будущих специалистов избегать ошибок приводящих к появлению уязвимостей.

Задачи:

Изучение классификации уязвимостей, OWASP TOP-10, атак. Приобритение навыка проводить pentest web-приложений. Фомирование навыков безопасной разработки программного обеспечения.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *С.1.Б.34 Защита программ и данных, С.1.Б.37 Техническая защита информации, С.1.Б.41.2 Анализ программных реализаций*

Постреквизиты дисциплины: *С.2.Б.П.2 Практика по получению профессиональных умений и опыта профессиональной деятельности, производственная практика (по специализации), С.2.Б.П.3 Преддипломная практика*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: способы и методы анализа алгоритмических решений для информационных систем и программного обеспечения. **Уметь:** анализировать используемые алгоритмы защиты информации в программном обеспечении. **Владеть:** навыками использования статических и динамических анализаторов, обратного инжиниринга.	ОПК-10 способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах
Знать: теоретические основы способов защиты программного обеспечения, требования к уровню защищенности программного обеспечения, основные принципы проведения pentest, технологии выявления уязвимостей. **Уметь:** применять теоретические знания на практике, анализировать полученные результаты. **Владеть:** практическими навыками использования утилит для проведения аудита безопасности.	ПК-9 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы
Знать: современные системы и методы защиты информации, политики безопасности в операционных системах, компьютерных сетях, базах данных. **Уметь:**	ПК-10 способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
оценивать уровень защищенности программного обеспечения, операционной системы, компьютерной сети, а так же эффективность работы средств защиты информации. **Владеть:** навыками выявления узких мест в программном обеспечении с помощью применения теоретических знаний и современных технологий.	компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
Знать: основные виды средств для проведения аудита безопасности и мониторинга компьютерных систем. **Уметь:** корректно настраивать и использовать средства для эффективного выявления уязвимостей. **Владеть:** базовыми навыками проведения аудита безопасности	ПК-11 способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации
Знать: основная классификация угроз безопасности, OWASP TOP-10, наиболее популярные атаки и способы взлома программного обеспечения, теоретический аспект политики безопасности. **Уметь:** формировать требования и используемые технологии к компьютерной системе. **Владеть:** знаниями для проведения корректной оценки эффективности работы системы безопасности, выявления недостатков и возможных угроз.	ПК-12 способностью проводить инструментальный мониторинг защищенности компьютерных систем
Знать: основные методы, принципы и архитектуры построения компьютерных сетей, web-приложений **Уметь:** использовать современные технологии при разработки программного обеспечения **Владеть:** навыками работы с различными средствами защиты информации	ПСК-2 способностью к освоению современных сред разработки программного обеспечения и новых образцов программных средств защиты в распределенных компьютерных системах

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 академических часов).

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	**180**	**180**
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

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Самостоятельная работа:	**118,75**	**118,75**
- выполнение индивидуального творческого задания (ИТЗ); *- выполнение расчетно-графического задания (РГЗ);* *- написание реферата (Р);* *- написание эссе (Э);* *- самостоятельное изучение разделов (перечислить);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к коллоквиумам;* *- подготовка к рубежному контролю и т.п.)*		
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 курс. Источники знаний и опыта. Основные понятия. Введение в безопасную разработку ПО. Принципы безопасности при проектировании ПО. Базовые виды уязвимостей ПО.	12	2			10
2	Классификация уязвимостей. OWASP Top-10.	14	2		2	10
3	SQL-инъекции. Внедрение операторов SQL. Виды инъекций. Техники внедрения.	20	4		6	10
4	OWASP A2-A6.	18	4		4	10
5	OWASP A7. XSS — Cross-Site Scripting.	30	4		6	20
6	Pentest Web-приложений.	30	6		4	20
7	Мастер-класс по экспуатации web-уязвимостей и защите от них.	28	4		4	20
8	Defensive Programming: методы разработки безопасного программного обеспечения.	28	4		4	20
	Итого:	180	30		30	120
	Всего:	180	30		30	120

4.2 Содержание разделов дисциплины

1. Введение в курс. Источники знаний и опыта. Основные понятия. Введение в безопасную разработку ПО. Принципы безопасности при проектировании ПО. Базовые виды уязвимостей ПО. Рекомендуемая литература. Основные понятия дисциплины. Безопасность ПО сегодня. Создание безопасных программ. Методика создания безопасного ПО. Безопасная эксплуатация ПО. Принципы безопасности при проектировании ПО. Базовые виды уязвимостей ПО.

2. Классификация уязвимостей. OWASP Top-10. Внедрение кода. SQL-инъекции. Инъекции кода. Некорректная аутентификация. Брутфорс пароля. Дублирование регистрации. Подделка cookies. Отсутствие защиты cookies от копирования. Утечка чувствительных данных. HTTP. Прослушивание данных. Wireshark. Небезопасное хранение данных. Использование устаревших методов хеширования. Внедрение внешних XML-сущностей. Внедрение опасных конструкций в XML. Нарушение контроля доступа. Отсутствие проверки авторизации при обращении к API. Выдача данных при замене ID. Доступ к учетной записи администратора при подмене URL.

Небезопасная конфигурация. Доступ к листингу файлов в директории. Просмотр исходных файлов приложения. Использование криптографически-слабых паролей. Межсайтовый скриптинг (XSS — Cross-Site Scripting). Внедрение и выполнение javascript-кода. CSRF. Небезопасная десериализация. Использование компонентов с известными уязвимостями. Отсутствие журналирования и мониторинга.

3. SQL-инъекции. Внедрение операторов SQL. Виды инъекций. Техники внедрения. Введение в тему безопасности web-приложений. Классическая техника эксплуатацииуязвимости. Внедрение операторов SQL (SQL Injection). Слепое внедрение операторов SQL (Blind SQL Injection). Работа с файловой системой при эксплуатации уязвимости SQL Injection. Выполнение команд на сервере при эксплуатации уязвимости SQL Injection. Методы обхода программных фильтров безопасности.

4. OWASP A2-A6. Некорректная аутентификация. Утечка сувствительных данных. Внедрение внешних XML-сущностей. Нарушение контроля доступа. Небезопасная конфигурация. Эксплуатируемость, распространенность, обнаруживаемость, влияние, виды уязвимостей, механизмы защиты, примеры использования.

5. OWASP A7. XSS — Cross-Site Scripting. Межмайтовый скриптинг. Эксплуатируемость. Распространенность. Обнаруживаемость. Влияние. Виды XSS по вектору атаки. Reflected XSS. Stored XSS. DOM XSS. Виды XSS по способу воздействия. Механизмы защиты.

6. Pentest Web-приложений. Общие понятия pentest. Виды тестирования. Подходы к тестированию. Поиск точек входа. URL. HTTP Request. HTTP Response. Этапы пентеста. Сбор информации. Популярные виды уязвимостей и атак. OWASP TOP 10. Broken Authentication. Виды уязвимостей. Утечка чувствительных данных: Sensitive Data Exposure. Внедрение внешних XML-сущностей. Broken Access Control. Security Misconfiguration. Межсайтовый скриптинг XSS — Cross-Site Scripting. Виды XSS. Демонстрация проведения pentest.

7. Мастер-класс по экспуатации web-уязвимостей и защите от них. SQL-инъекции. Использование утилиты SQLMap. Эксплуатация простой SQL-инъекции UNION Query в GET-параметре. Эксплуатация SQL-инъекции BLIND Boolean Based. Command Injection. Инъкция с выводом результата выполнения команды. Blind Command Injection. Server-Side Includes (SSI). Directory Traversal. File Traversal. LFI/RFI. XXE.

8. Defensive Programming: методы разработки безопасного программного обеспечения. Безопаснвй дизайн. Безопасная архитектура. Качество кода. Валидация данных. Преждевременная оптимизация. Unit tests. Модульные тесты. Интеграционное тестирование. Системное тестирование. Test-driven development. Code review. Отказоустойчивость приложения. Избыточность. Балансировка нагрузки. Защитное программирование. Модели синхронизации. Количественные метрики. Системные метрики. Лог-файлы.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2	Реализация уязвимости «переполнение буфера».	2
2	3	Поиск SQL-инъекций в web-приложении.	2
3	3	Внедрение SQL — уязвимостей.	4
4	4	Внедрение Broken Authentication, Sensitive Data Exposure, Broken Access Control, XXE. Внедрение способов защиты от уязвимостей.	4
5	5	Поиск XSS-уязвимостей.	2
6	5	Внедрение XSS уязвимостей.	4
7	6	Pentest web-приложения.	4
8	7	Поиск web-уязвимостей.	4
9	8	Разработка защищенного прототипа сервиса.	4
		Итого:	30

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Галатенко В. А. Основы информационной безопасности [Электронный ресурс] / Галатенко В. А. - Интернет-Университет Информационных Технологий, 2006. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=233063

2. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]. – М.: ДМК Пресс, 2010. – 544 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=86475&sr=1

3. Кучеренко, В. Ассемблер [Текст] : тонкости, хитрости и секреты программирования / В. Кучеренко. - М. : Майор, 2001. - 160 с. - (Мой компьютер). - Библиогр.: с. 156. - ISBN 5-901321-06-5.

4. Торстейнсон, П. Криптография и безопасность в технологии. NET [Текст] / П.Торстейнсон, Г. А. Ганеш; пер. с англ. В. Д. Хорева ; под ред. С. М. Молявко. - М. : Бином, 2007. -480 с. : ил. - Предм. указ.: с. 448-472. - ISBN 978-5-94774-312-8.

5.2 Дополнительная литература

1. Галатенко В. А. Основы информационной безопасности [Электронный ресурс] / Галатенко В. А. - Интернет-Университет Информационных Технологий, 2006. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=233063

2. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]. – М.: ДМК Пресс, 2010. – 544 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=86475&sr=1

3. Кучеренко, В. Ассемблер [Текст] : тонкости, хитрости и секреты программирования / В. Кучеренко. - М. : Майор, 2001. - 160 с. - (Мой компьютер). - Библиогр.: с. 156. - ISBN 5-901321-06-5.

4. Торстейнсон, П. Криптография и безопасность в технологии. NET [Текст] / П. Торстейнсон, Г. А. Ганеш; пер. с англ. В. Д. Хорева ; под ред. С. М. Молявко. - М. : Бином, 2007. - 480 с. : ил. - Предм. указ.: с. 448-472. - ISBN 978-5-94774-312-8.

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

1. Операционная система Microsoft Windows.
2. Пакет настольных приложений Microsoft Office (Word, Excel, PowerPoint).
3. Среда разработки Microsoft Visual Studio.
4. Операционная система Kali Linux.
5. Утилиты: SQLMap, Netdiscover, Nmap, Hydra, Dirb.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского 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 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.