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.41.2 Анализ программных реализаций»

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 — *должность* — *подпись* — К. К. Шпинёв *расшифровка подписи*

_____ — *должность* — *подпись* — *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность — *код наименование* — *личная подпись* — И.В.Влацкая *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 у студентов теоретических знаний, практических навыков в анализе программных решений, компетенций и целостных представлений об основах построения архитектур, моделей. Изучение технологий анализа программ и приобретение навыка самостоятельного анализа любых алгоритмических решений.

Задачи:

- изучение теоретических основ архитекрутных решений программных продуктов;
- получение навыка применения статического и динамического анализа, а также использования обратного инжиниринга при анализе программных реализаций;
- изучение методов обфускации программ;
- получение навыков работы с бинарным кодом: осуществление тестирования и отладки;
- получение теоретических знаний обеспечения безопасности web-приложений согласно OWASP.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *С.1.Б.22 Языки программирования, С.1.Б.23 Методы программирования*

Постреквизиты дисциплины: *С.1.Б.41.3 Уязвимость программного обеспечения, С.1.Б.41.7 Параллельное программирование*

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: - методы построения моделей и алгоритмов; - методы анализа программных реализаций; **Уметь:** - использовать инструменты для обратного инжиниринга, обфускации, анализа программ; - применять утилиты для анализа программных реализаций и алгоритмов к реальным задачам; **Владеть:** - навыками обратного инжиниринга программных реализаций;	ОПК-10 способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах
Знать: Теоретические основы построения архитектур, моделей, алгоритмов программных продуктов, операционных систем, систем антивирусной защиты, баз данных и компьютерных сетей. Знать теоретический аспект OWASP. Теоретические основы сетевых протоколов. **Уметь:** Оценивать эффективность систем защиты информации в программных продуктах и компьютерных системах. Оценивать степень защищенность системы. Использовать классификацию OWASP, применяя к реальным задачам. **Владеть:** Навыками использования средств защиты веб-приложений согласно	ПК-10 способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
OWASP. Навыками использования средств криптографической защиты. Навыками применения сетевых протоколов.	информации
Знать: Основные принципы обфускации программного кода, статического и динамического анализа. Основные методы работы с бинарным кодом приложений. **Уметь:** Применять утилиты для анализа бинарного кода. Настраивать инструменты для статического и динамического анализа кода. Применять методы обфускации приложений для дополнительной защиты программного кода. **Владеть:** Навыками использования утилит для анализа бинарного кода, обфускации и статических и динамических анализаторов.	ПСК-1 способностью использовать современные технологии программирования для разработки защищенного программного обеспечения
Знать: Принципы работы компьютерных и операционных систем и современные применяемые способы защиты информации. **Уметь:** Использовать современные средства для создания и разработки программного обеспечения. **Владеть:** Навыками разработки сетевого программного обеспечения с применением современных технологий защиты.	ПСК-2 способностью к освоению современных сред разработки программного обеспечения и новых образцов программных средств защиты в распределенных компьютерных системах
Знать: Основные принципы защиты web-приложений, основные используемые уязвимости в web-приложениях. **Уметь:** Находить уязвимости в программном обеспечении, используя современные утилиты и теоретические основы проектирования архитектур приложений. **Владеть:** Навыками поиска уязвимостей и недокументированных возможностей в программном обеспечении.	ПСК-4 способностью проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**47,25**	**47,25**
Лекции (Л)	16	16
Лабораторные работы (ЛР)	30	30
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа:	**60,75**	**60,75**
- выполнение индивидуального творческого задания (ИТЗ); *- выполнение расчетно-графического задания (РГЗ);*		

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
- 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 6 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Жизненный цикл программы. Статический и динамический анализ. Тестирование и отладка. Анализ бинарного кода.	21	2		4	15
2	Pentest Web-приложений. Тестирование. OWASP. Некорректная аутернтификация. Утечка чувствитеных данных. Внедрение внешних XML-сущностей. Нарушение контроля доступа. Небезопасная конфигурация. Межсайтовый скриптинг.	20	4		4	12
3	Обфускация. Цели, виды, назначение. Деобфускация. Нормализация кода. Утилиты.	16	2		4	10
4	Краткий обзор основных уязвимостей программного обеспечения. Демонстрация.	16	4		2	10
5	Практическое применение знаний. Разбор реальных задач. CTF.	35	4		16	15
	Итого:	108	16		30	62
	Всего:	108	16		30	62

4.2 Содержание разделов дисциплины

1. Жизненный цикл программы. Статический и динамический анализ. Тестирование и отладка. Анализ бинарного кода. Жизненный цикл программы. Анализ программ. Динамический анализ. Статический анализ. Статический анализ для обнаружения дефектов кода. Нефункциональные дефекты. Проявление дефектов. Опасные конструкции. Инструменты статического анализа. Общая модель работы анализатора. Отчёт об ошибках. Модели программы. Требования к моделям. Типы моделей программ. Классы обнаружения ошибок. Путь распространения ошибки. Место статического анализа при разработке ПО. Тестирование и отладка. «Борбаги» и «гейзенбаги». Отладка пользовательского кода. Отладочная информация. Форматы отладочной информации. Базовый функционал отладчика. Аппаратная поддержка отладки. Антиотладочные приемы. Анализ бинарного кода. Исходный и бинарный код. Компиляция как процесс потери информации. Общая схема анализа бинарного кода. Получение предмета анализа. Восстановление абстракций, необходимых для анализа. Бинарный код: начальное представление. Выделение инструкций. Выделение опкодов и операндов. Задачи декомпиляции. Инструменты анализа бинарных программ. Дизассемблирование. Декомпиляция. Трассировка. Практическая часть.

2. Pentest Web-приложений. Тестировнаие. OWASP. Некорректная аутернтификация. Утечка чувствитеных данных. Внедрение внешних XML-сущностей. Нарушение контроля доступа. Небезопасная конфигурация. Межмайтовый скриптинг. Что такое 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.

3. Обфускация. Цели, виды, назначение. Деобфускация. Нормализация кода. Утилиты. Обфускация. Цели обфускации. Виды обфускации. Лексическая обфускация. Обфускация данных. Обфускация потока управления. Превентивная обфффускация. Методы деобфускации. Нормализация кода перед деобфускацией. Деобфускаторы.

4. Краткий обзор основных уязвимостей программного обеспечения. Демонстрация. 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.

5. Практическое применение знаний. Разбор реальных задач. CTF. Программные реализации, включающие криптографию: кодировки, классические шифры, одноразовый блокном, асимметричное шифрование. Хеширование. Примеры хеш-функций. Крипрограффическая хеш-функция. Коллизии. Часто используемые хеш-функции. Сравнение хеш-функций. Процесс вычисление хеша. MD5. MAC. Length extension attack. Хранение паролей. Bcrypt. SHA-*. Взлом хешей. Задачи.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Анализ программных реализаций с помощью инструментов анализа бинарного кода.	4
2	2	Поиск уязвимостей в web-приложениях .	4
3	3	Обфускация кода программных реализаций.	4
4	4	Настройка среды и инструментов для поиска уязвимостей.	2
5	5	Реализация и эксплуатация уязвимости «переполнение буфера»	4
6	5	Поиск уязвимостей в web-server.	6
7	5	CTF: взлом игрового образа.	6
		Итого:	30

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. 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

2. Макаров А. В. Common Intermediate Language и системное программирование в Microsoft.NET [Электронный ресурс] / Макаров А. В., Скоробогатов С. Ю., Чеповский А. М. - Интернет-Университет Информационных Технологий, 2006. – Режим доступа:http://biblioclub.ru/index.php?page=book&id=233196&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.

5.2 Дополнительная литература

1. Касперски, К. Искусство дизассемблирования [Комплект] / К. Касперски, Е. Рокко. - СПб. : БВХ-Петербург, 2008. - 896 с. : ил. + 1 электрон. опт. диск (CD-ROM). - Предм. указ.: с. 875. - ISBN 978-5-9775-0082-1.

2. Виега Д. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок [Электронный ресурс] / Виега Д., Лебланк Д., Ховард М. - ДМК Пресс, 2009. – Режим доступа: http://www.biblioclub.ru/index.php?page=book&id=130996

5.3 Периодические издания

1. Информационная безопасность : журнал. - М. : Агентство "Роспечать".

2. Информация и безопасность : журнал. - М. : Агентство "Роспечать".

3. Вестник информационной безопасности : журнал. - М. : Агенство "Роспечать".

5.4 Интернет-ресурсы

1. Чернов А.В. Анализ запутывающих преобразований программ. – Режим доступа: http://citforum.ru/security/articles/analysis/

2. Wireshark — приручение акулы. – Режим доступа: https://habrahabr.ru/company/pentestit/blog/204274/

3. Sysinternals Learning Resources. – Режимдоступа: https://docs.microsoft.com/en-us/sysinternals/learn/

4. CTF на физтехе. Кодировки. Классические шифры. Симметричное шифрование. Атаки. - Режим доступа: https://github.com/xairy/mipt-ctf/tree/master/02-crypto/01-symmetric

5. CTF на физтехе. Хеширование. Криптографическая хеш-функция. Атаки - Режим доступа: https://github.com/xairy/mipt-ctf/tree/master/02-crypto/03-hashing

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.