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.44.2 Анализ программных реализаций»

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 2023

Рабочая программа дисциплины «*Б1.Д.Б.44.2 Анализ программных реализаций*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 7 от "9" марта 2023 г.

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

Исполнители:
доцент *должность* *подпись* И.В. Влацкая *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 формирования фонда и научной обработки документов
личная подпись Н.Н. Бигалиева *расшифровка подписи* С.А. Бикташева

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

№ регистрации _____

© Влацкая И.В., 2023
© ОГУ, 2023

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:
Изучение теоретических основ и технологий анализа программ и реализованных алгоритмических решений.

Задачи:
- изучение основ обратного инжиниринга программ;
- изучение методов обфускации программ;
- изучение методов профилировки программ;
- изучение методов статического анализа кода.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.22 Языки программирования, Б1.Д.Б.23 Методы программирования*

Постреквизиты дисциплины: *Б1.Д.Б.44.3 Уязвимость программного обеспечения, Б1.Д.Б.44.7 Параллельное программирование*

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 инструментальных средств отладки и дизассемблирования программного кода	**Знать:** -классы угроз безопасности; -основные уязвимости программного обеспечения; -системы оценивания рисков; средства защиты Web-приложений. **Уметь:** - выявлять уязвимости в разрабатываемом программном обеспечении; - выявлять возможности для SQL-инъекций; -оценивать возможности для XSS- и CSRF- атак. **Владеть:** навыками проведения по проведению сертификации средств

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		защиты информации; - навыками дизассемблирования программного кода; - навыками использования инструментальных средств тестирования и дизассемблирования.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов	
	6 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: *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным работам;* *- подготовка к коллоквиумам;* *- подготовка к рубежному контролю и т.п.)*	**82,75**	**82,75**
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	Введение, декомпиляция и дизассемблирование программ	32	6		8	18
2	Обфускация программ	34	4		8	22
3	Мониторинг активности программ, перехват сетевых пакетов	36	8		6	22
4	Статический и динамический анализ программ	42	12		8	22
	Итого:	144	30		30	84
	Всего:	144	30		30	84

4.2 Содержание разделов дисциплины

1. Введение, декомпиляция и дизассемблирование программ. *Анализ программных реализаций. Понятие обратного инжиниринга программ, его назначение. Методики обратного инжиниринга: дизассемблирование машинного кода, декомпиляция байтового кода и обратный инжиниринг потоков данных. Принципы работы с декомпиляторами и дизассемблерами.Типичные действия злоумышленника, занимающегося взломом защиты.*

2. Обфускация программ. *Понятие обфускации программ. Типовые методы обфускации программ: обфускация переменных, обфускация потока управления, использование динамических прокси для методов, сжатие и шифрование ресурсов, шифрование строк, отсечение кода, слияние сборов. Принципы работы с существующими инструментами для обфускации программ.*

3. Мониторинг активности программ, перехват сетевых пакетов. *Анализ программ на основе мониторинга их работы. Использование инструментов пакета Sysinternals Suit для мониторинга обращения к файлам, реестру, сетевых потоков данных и прописывания программ для автозапуска в Windows. Основные понятия анализаторов сетевого трафика (снифферов), их назначение, принципы работы, места установки в сети. Использование анализаторов сетевого трафика для перехвата конфиденциальных данных, подмены информации, обратного инжиниринга сетевых протоколов. Примеры использования программ WireShark и RawCap. Применение инструмента Fiddler для анализа HTTP-трафика приложений. Принципы работы, основные его возможности по перехвату HTTP запросов и ответов, их отображению, декодированию, фильтрации, модификации, генерации запросов и ответов. Примеры использования. Написание сетевых приложений для протоколов TCP/IP и HTTP средствами библиотеки языка программирования.*

4. Статический и динамический анализ программ. *Статический анализ кода. Основные понятия, принципы работы, области использования. Инструменты для статического анализа. Типовые ошибки, обнаруживаемые с помощью статического анализа. Динамический анализ программ. Этапы анализа, способы взаимодействия с проверяемой программой, результаты анализа, области применения, достоинства и недостатки. Профилирование программ, как инструмент динамического анализа. Совместное использование статического и динамического анализа программ.*

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Обратный инжиниринг приложений	8
2	2	Обфускация приложений	4
3	3	Мониторинг активности программ	6
4	4	Статические анализаторы кода	6
5	4	Профилирование программ	6
		Итого:	30

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. 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.
2. Буйневич М.В, Израидов К.Е., Красов А.В. Защита программ и данных. Часть 1:Способы анализа данных.Учебное пособие СПб ГУТ, Санкт-Петербург,2020г. Режим доступа: https://e.lanbook.com/book/180081

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.

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. – Режим доступа: https://docs.microsoft.com/en-us/sysinternals/learn/
4. Галатенко, В. Основы информационной безопасности // Национальный открытый университет «Интуит», 2012. – Режим доступа: http://www.intuit.ru/studies/courses/10/10/info

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

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. Среда разработки Microsoft Visual Studio.

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 лаборатория «*Наименование*» (при наличии), (компьютерный класс) оснащенная/ оснащенный (указывается конкретное оборудование и т.п.)

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.