МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Технология реверс-инжиниринга

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью дисциплины "Технология реверс-инжиниринга" является приобретение знаний, навыков и умений реверс инжиниринга с целью формирования соответствующих компетенций.

Задачами дисциплины:

- приобретение навыков и умений решения задач реверс инжиниринга с использованием различного инструментария, а именно: отладчиков, дизассемблеров, вспомогательных утилит, средств статического анализа;
- приобретение знаний, навыков и умений, позволяющих выявлять уязвимости программного обеспечения с использованием технологий реверс инжиниринга;
- приобретение знаний, навыков и умений, необходимых для оценки рисков, связанных с выявленными с использованием технологий реверс инжиниринга уязвимостей программного обеспечения;
- приобретение знаний, навыков и умений, необходимых для парирования выявленных с использованием технологий реверс инжиниринга уязвимостей программного обеспечения.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-2 - Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;

ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ОПК-12 - Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения;

ПК-4 - Способен участвовать в разработке подсистемы информационной безопасности компьютерной (в том числе автоматизированной) системы включая разработку программно-аппаратных средств защиты информации, защищенных операционных систем, систем

управления базами данных, компьютерных сетей, систем антивирусной защиты, средств криптографической защиты информации.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- Современное программное обеспечение системного и прикладного назначения, включая отладчики, дизассемблеры и средства статического/динамического анализа, необходимые для реверс-инжиниринга.
- Основные нормативные правовые акты и нормативно-методические документы ФСБ России и ФСТЭК России, регламентирующие защиту информации и требования к безопасности программного обеспечения.
- Архитектуру операционных систем, принципы управления процессами, памятью и файловыми системами, необходимые для анализа поведения приложений.
- Методы и средства реверс-инжиниринга, позволяющие выявлять недекларированные возможности, закладки и уязвимости в программном обеспечении.

Уметь:

- Оценивать функциональные возможности и выбирать программные средства (отечественного и зарубежного производства) для эффективного решения задач обратной разработки.
- Соотносить выявленные в ходе реверс-инжиниринга уязвимости с требованиями нормативных документов для оценки их критичности.
- Анализировать и восстанавливать алгоритмы работы прикладного и системного программного обеспечения на основе его машинного кода.
- Анализировать защищенность существующих программных решений и формулировать требования к разработке более надежных и защищенных компонентов.

Владеть:

- Навыками применения специализированного инструментария (x64dbg, IDA Pro, Radare2, Frida и др.) для анализа и исследования программного кода.
- Методами оценки рисков, связанных с выявленными уязвимостями программного обеспечения, и способами обоснования необходимости их парирования в соответствии с нормативными требованиями.
- Навыками отладки и трассировки программ для выявления причин сбоев и восстановления логики их работы.

- Навыками применения технологий обратной разработки для тестирования (пентеста) и аудита безопасности программно-аппаратных средств защиты информации.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №6
Контактная работа при проведении учебных занятий (всего):	80	80
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	48	48

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 28 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Введение Рассматриваемые вопросы: - Основные понятия обратной разработки программной разработки.
2	Методики проведения обратной разработки Рассматриваемые вопросы: - анализ обмена данными приложения с помощью различных анализаторов трафика; - использование режима отладки для поиска нужных участков кода и просмотра данных, с которыми работает приложение; - дизассемблирование машинного кода программы (изучение требует довольно много времени); - декомпиляция кода программы для создания исходного кода программы на языке программирования высокого уровня.
3	Средства обратной разработки программной разработки Рассматриваемые вопросы: - отладчики для реверс-инжиниринга 1) x64dbg 2) WinDbg 3) OllyDbg
4	Дизассемблеры для реверс-инжиниринга Рассматриваемые вопросы: - IDA Disassembler - Radare2
5	Вспомогательные утилиты для реверс-инжиниринга Рассматриваемые вопросы: - Detect it Easy (DiE) - ExeInfoPE - HxD - HIEW - Pestudio - PE-bear - Fakenet-NG - ProcessExplorer - RegShot - TCPView - Resource Hacker
6	Средства статического анализа Рассматриваемые вопросы: - Jadx - Apktool - APKiD - Simplify - DeGuard - Bytecode Viewer - QARK - AK-BC
7	Средства динамического анализа Рассматриваемые вопросы: - Frida - Objection - Inspeckage

№ п/п	Тематика лекционных занятий / краткое содержание
	- Drozer - АК-ВС

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Средства обратной разработки. Отладчик x64dbg. Изучение интерфейса и базовых возможностей отладчика x64dbg. Выполнение трассировки простой программы, установка точек останова, анализ регистров и стека.
2	Средства обратной разработки. Отладчик WinDbg. Освоение работы с отладчиком WinDbg для анализа пользовательских приложений и драйверов режима ядра. Изучение команд для отображения информации о процессе и памяти.
3	Средства обратной разработки. Отладчик OllyDbg. Знакомство с классическим отладчиком OllyDbg. Анализ защит простых исполняемых файлов, поиск и модификация ключевых участков кода.
4	Дизассемблеры. IDA Disassembler. Основы работы в IDA Pro. Навигация по дизассемблированному коду, работа с графами потоков управления, идентификация библиотечных функций.
5	Дизассемблеры. Radare2. Изучение основ работы в консольном дизассемблере Radare2. Навигация, анализ кода, использование скриптов для автоматизации.
6	Вспомогательные утилиты для реверс-инжиниринга. Комплексное исследование файла. Определение упаковщиков (DiE), просмотр и редактирование ресурсов (Resource Hacker), мониторинг активности (Process Explorer, RegShot, TCPView).
7	Статический анализ Android-приложений. Jaxx. Основы работы с Jaxx. Анализ манифеста, декомпиляция исходного кода приложения для поиска потенциальных уязвимостей.
8	Статический анализ Android-приложений. Apktool. Декомпиляция и повторная сборка Android-приложения с помощью Apktool. Анализ и модификация ресурсов и Smali-кода.
9	Статический анализ Android-приложений. APKiD. Использование APKiD для быстрого сканирования APK-файлов на наличие обфускаторов, трейсеров и других подозрительных компонентов.
10	Статический анализ Android-приложений. Simplify. Применение Simplify для автоматического упрощения (деобфускации) запутанного кода Android-приложений с целью облегчения его анализа.
11	Статический анализ Android-приложений. DeGuard. Сравнительный анализ онлайн-сервиса DeGuard с локальными средствами для декомпиляции и поиска уязвимостей.
12	Статический анализ Android-приложений. Bytecode Viewer. Комплексный анализ Android-приложения с использованием Bytecode Viewer для работы с несколькими декомпиляторами одновременно.
13	Статический анализ Android-приложений. QARK. Автоматизированный поиск уязвимостей безопасности в Android-приложениях с помощью инструмента QARK и анализ полученного отчета.

№ п/п	Наименование лабораторных работ / краткое содержание
14	Динамический анализ. Frida. Objection. Введение в динамическую инструментовку. Использование Frida и Objection для перехвата вызовов функций и обхода базовых защит на лету.
15	Динамический анализ. Inspeckage. Использование Inspeckage для динамического анализа Android-приложений: мониторинг файловой активности, сетевых запросов, логов и Shared Preferences.
16	Динамический анализ. Drozer. Поиск уязвимостей в межкомпонентном взаимодействии (IPC) Android-приложений с помощью фреймворка Drozer.
17	Комплексный анализ. AK-BC. Изучение возможностей инструмента AK-BC как комбинированного средства для статического и динамического анализа Android-приложений.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к лабораторным работам.
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Анализ вредоносных программ Монаппа К.А. Книга М.: ДМК Пресс, - 452 с. - ISBN 78-5-97060-700-8 , 2019	https://reader.lanbook.com/book/123709#5
2	Введение в защиту компьютерной информации Климентьев К.Е. Учебное пособие Министрерство науки и высшего образования, Самарский университет. - Самара: Издательство Самарского университета, - 183 с. - ISBN 978-5-7883-1526-3 , 2020	https://reader.lanbook.com/book/189043#2

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

Электронно-библиотечная система ibooks.ru (http://ibooks.ru/).

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Зачет в 6 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

профессор, профессор, д.н. кафедры «Управление и защита информации» В.Г. Сидоренко

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин