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:

Основные нормативные правовые акты и нормативно методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю. Современное программное обеспечение системного и прикладного назначения.

Уметь:

Оценивает функциональные возможности аппаратных и программных средств, включая операционные системы, в составе компьютерной системы; проводит классификацию и устанавливает групповую принадлежность программного обеспечения. Строит, анализирует и реализует алгоритмы, в том числе криптографические, в современных программных комплексах. Проектирует и разрабатывает компоненты защищенных автоматизированных систем в сфере профессиональной деятельности.

Владеть:

Выполняет работы по установке, настройке, администрированию и проверке работоспособности программно-аппаратные средства системного, прикладного и специального назначения в сфере профессиональной деятельности.

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 1
Контактная работа при проведении учебных занятий (всего):	84	84
В том числе:		
Занятия лекционного типа	34	34
Занятия семинарского типа	50	50

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 24 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

№ п/п	Тематика лекционных занятий / краткое содержание
	- 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 - АК-ВС
7	Средства динамического анализа Рассматриваемые вопросы: - Frida - Objection - Inspeckage - Drozer - АК-ВС

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	ЛР №1 Средства обратной разработки программной разработки. x64dbg.
2	ЛР №2 Средства обратной разработки программной разработки. WinDbg.
3	ЛР №3 Средства обратной разработки программной разработки. OllyDbg.
4	ЛР №4 Дизассемблеры для реверс-инжиниринга. IDA Disassembler.
5	ЛР №5 Дизассемблеры для реверс-инжиниринга. Radare2.
6	ЛР №6 Вспомогательные утилиты для реверс-инжиниринга.
7	ЛР №7 Средства статического анализа. Jadx
8	ЛР №8 Средства статического анализа. Apktool

№ п/п	Наименование лабораторных работ / краткое содержание
9	ЛР №9 Средства статического анализа. APKiD.
10	ЛР №10 Средства статического анализа. Simplify.
11	ЛР №11 Средства статического анализа. DeGuard.
12	ЛР №12 Средства статического анализа. Bytecode Viewer.
13	ЛР №13 Средства статического анализа. QARK.
14	ЛР №14 Средства динамического анализа. Frida. Objection.
15	ЛР №15 Средства динамического анализа. Inspeckage
16	ЛР №16 Средства динамического анализа. Drozer
17	ЛР №17 Средства анализа. AK-BC

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	Подготовка к промежуточной аттестации.
6	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Assembler В.И. Юров Однотомное издание "Питер" , 2008	НТБ (уч.3)
2	Разработка приложений на языке Ассемблер для МП Intel В.А. Варфоломеев; МИИТ. Каф. "Автоматизированные системы управления" Однотомное издание МИИТ , 2006	НТБ (ЭЭ); НТБ (уч.4)
3	Технология подготовки и отладки ассемблерных программ Ларина Т.Б., Каф. Вычислительные	НТБ Электронный экземпляр http://www.miit.ru

	системы и сети Однотомное издание МИИТ , 2014	
4	Методические указания к лабораторным работам по дисциплине “Программирование на языке ассемблера” Шейкина Г.А. МИИТ , 2004	НТБ Электронный экземпляр http://www.miit.ru
5	Реверсинг и защита программ от взлома Панов А. Санкт-Петербург: БХВ-Петербург , 2006	https://ibooks.ru/products/333573

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

Для проведения аудиторных занятий и самостоятельной работы требуется:

1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET и INTRANET.

2. Компьютерный класс с кондиционером. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANET

Для проведения практических занятий:

компьютерный класс; кондиционер; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

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