МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

26 мая 2020 г.

Кафедра «Управление и защита информации»

Автор Сидоренко Валентина Геннадьевна, д.т.н., профессор

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Технология реверс-инжиниринга

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2020

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 26 мая 2020 г. Председатель учебно-методической комиссии С.В. Володин	Протокол № 16 21 мая 2020 г. Заведующий кафедрой Л.А. Баранов

Москва 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью дисциплины 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. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Технология реверс-инжиниринга" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

2.1. Наименования предшествующих дисциплин

2.2. Наименование последующих дисциплин

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ОПК-2 Способен применять программные средства системного и прикладного назначения для решения профессиональных задач;	ОПК-2.1 Оценивает функциональные возможности аппаратных и программных средств, включая операционные системы, в составе компьютерной системы; проводит классификацию и устанавливает групповую принадлежность программного обеспечения. ОПК-2.2 Выполняет работы по установке, настройке, администрированию и проверке работоспособности программно-аппаратные средства системного, прикладного и специального назначения в сфере профессиональной деятельности. ОПК-2.3 Выполняет управление инцидентами безопасности при функционировании программных средств системного, прикладного и специального назначения.
2	ОПК-6 Способен анализировать и учитывать текущее состояние и тенденции развития методов криптографической защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, средств технической защиты информации, сетей и систем передачи информации при решении профессиональных задач;	ОПК-6.1 Строит, анализирует и реализует алгоритмы, в том числе криптографические, в современных программных комплексах. ОПК-6.2 Строит, анализирует и реализует протоколы, в том числе криптографические, в современных программных комплексах. ОПК-6.3 Строит, анализирует и учитывает новые методы защиты в системах управления базами данных, сетей и систем передачи информации.
3	ОПК-12 Способен участвовать в разработке программно-аппаратных средств защиты информации компьютерных систем и сетей;	ОПК-12.1 Участвует в разработке программно-аппаратных средств защиты информации компьютерных систем и сетей.
4	ПКО-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.	ПКО-4.1 Осуществляет рациональный выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности, создаваемых защищенных компьютерных систем в сфере профессиональной деятельности. ПКО-4.2 Проектирует и разрабатывает компоненты защищенных автоматизированных систем в сфере профессиональной деятельности.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

4.1. Общая трудоемкость дисциплины составляет:

3 зачетные единицы (108 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 8
Контактная работа	48	48,15
Аудиторные занятия (всего):	48	48
В том числе:		
лекции (Л)	16	16
лабораторные работы (ЛР)(лабораторный практикум) (ЛП)	32	32
Самостоятельная работа (всего)	60	60
ОБЩАЯ трудоемкость дисциплины, часы:	108	108
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.0	3.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК2, ТК	ПК2, ТК
Виды промежуточной аттестации (экзамен, зачет)	Зачет	Зачет

4.3. Содержание дисциплины (модуля), структурированное по темам (разделам)

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	8	Раздел 1 Введение	2					2	
2	8	Тема 1.1 Основные понятия обратной разработки программной разработки.	2					2	
3	8	Раздел 2 Методики проведения обратной разработки	2				20	22	
4	8	Тема 2.1 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.	2				20	22	
5	8	Раздел 3 Средства обратной разработки программной разработки	2	4				6	
6	8	Тема 3.1 Отладчики для реверс-инжиниринга 1) x64dbg 2) WinDbg 3) OllyDbg	2	4				6	ПК2
7	8	Раздел 4 Дизассемблеры для	2	6			20	28	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		реверс-инжиниринга							
8	8	Тема 4.1 IDA Disassembler - Radare2	2	6			20	28	
9	8	Раздел 5 Вспомогательные утилиты для реверс-инжиниринга	4	6				10	
10	8	Тема 5.1 Detect it Easy (DiE) ExeInfoPE; HxD; HIEW; Pestudio; PE-bear; Fakenet-NG; ProcessExplorer; RegShot; TCPView; Resource Hacker;	4	6				10	ТК
11	8	Раздел 6 Средства статического анализа	2	8				10	
12	8	Тема 6.1 Jadx Apktool; APKiD; Simplify; DeGuard; Bytecode Viewer; QARK; АК-ВС.	2	8				10	
13	8	Раздел 7 Средства динамического анализа	2	8			20	30	Зачет
14	8	Тема 7.1 Frida Objection; Inspeckage; Drozer; АК-ВС.	2	8			20	30	
15		Всего:	16	32			60	108	

4.4. Лабораторные работы / практические занятия

Практические занятия учебным планом не предусмотрены.

Лабораторные работы предусмотрены в объеме 32 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	8	РАЗДЕЛ 3 Средства обратной разработки программной разработки Тема: Отладчики для реверс-инжиниринга	Средства обратной разработки программной разработки. x64dbg. WinDbg. OllyDbg.	4
2	8	РАЗДЕЛ 4 Дизассемблеры для реверс-инжиниринга Тема: IDA Disassembler	Дизассемблеры для реверс-инжиниринга. IDA Disassembler. Radare2.	6
3	8	РАЗДЕЛ 5 Вспомогательные утилиты для реверс-инжиниринга Тема: Detect it Easy (DiE)	Вспомогательные утилиты для реверс-инжиниринга.	6
4	8	РАЗДЕЛ 6 Средства статического анализа Тема: Jadx	Средства статического анализа. Jadx. Apktool. APKiD. Simplify. DeGuard. Bytecode Viewer. QARK.	8
5	8	РАЗДЕЛ 7 Средства динамического анализа Тема: Frida	Средства динамического анализа. Frida. Objection. Inspeckage. Drozer. АК-ВС.	8
			ВСЕГО:	32/0

4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы (проекты) не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Технология реверс-инжиниринга» осуществляется в форме лекций и лабораторных работ.

Лабораторные работы организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач). Остальная часть практического курса проводится с использованием интерактивных (диалоговые) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения, а также использованием компьютерной тестирующей системы.

Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям относится отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов.

Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 6 разделов, представляющих собой логически завершенный объём учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые опросы, решение тестов с использованием компьютеров или на бумажных носителях.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы	Всего часов
1	2	3	4	5
1	8	РАЗДЕЛ 2 Методики проведения обратной разработки Тема 1: Анализ обмена данными приложения с помощью различных анализаторов трафика.	СР №1 1. Подготовка к прохождению промежуточному контроля. 2. Повторение лекционного материала. 3. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 4. Конспектирование изученного материала.	20
2	8	РАЗДЕЛ 4 Дизассемблеры для реверс-инжиниринга Тема 1: IDA Disassembler	СР №2 1. Подготовка к прохождению текущего контроля. 2. Повторение лекционного материала. 3. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 4. Конспектирование изученного материала.	20
3	8	РАЗДЕЛ 7 Средства динамического анализа Тема 1: Frida	СР №3 1. Повторение лекционного материала. 2. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 3. Конспектирование изученного материала. 4. Подготовка к зачету.	20
			ВСЕГО:	60

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
1	Assembler	В.И. Юров	"Питер", 2008 НТБ (уч.3)	Все разделы
2	Разработка приложений на языке Ассемблер для МП Intel	В.А. Варфоломеев; МИИТ. Каф. "Автоматизированные системы управления"	МИИТ, 2006 НТБ (ЭЭ); НТБ (уч.4)	Все разделы
3	Технология подготовки и отладки ассемблерных программ	Ларина Т.Б., Каф. Вычислительные системы и сети	МИИТ, 2014 НТБ Электронный экземпляр http://www.miit.ru	Все разделы
4	Методические указания к лабораторным работам по дисциплине “Программирование на языке ассемблера”	Шейкина Г.А.	МИИТ, 2004 НТБ Электронный экземпляр http://www.miit.ru	Все разделы
5	Реверсинг и защита программ от взлома	Панов А.	Санкт-Петербург: БХВ-Петербург, 2006 https://ibooks.ru/products/333573	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ 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 3. Для проведения практических занятий: компьютерный класс; кондиционер; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Microsoft Internet Explorer (или другой браузер).
Операционная система Microsoft Windows.
Microsoft Office.

10. 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.

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Обучающимся необходимо помнить, что качество полученного образования в немалой степени зависит от активной роли самого обучающегося в учебном процессе. Обучающийся должен быть нацелен на максимальное усвоение подаваемого лектором материала, после занятий и во время специально организуемых индивидуальных встреч он может задать лектору интересующие его вопросы. Выполнение практических заданий и лабораторных работ служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике. Они способствуют развитию самостоятельности обучающихся, более активному освоению учебного материала, являются важной предпосылкой формирования профессиональных качеств будущих специалистов. При подготовке специалиста важны не только серьезная теоретическая подготовка, знание основ программирования и алгоритмизации, но и умение ориентироваться в разнообразных практических ситуациях, ежедневно возникающих в его деятельности. Этому способствует форма обучения в виде практических занятий. Задачи практических занятий закрепление и углубление знаний, приобретенных в процессе самостоятельной работы с учебной литературой, формирование у обучающихся умений и навыков работы с исходными данными, научной литературой и специальными документами Самостоятельная работа может быть успешной при определенных условиях, которые необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности. Каждому студенту следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтра. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что- то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана. Компетенции обучающегося, формируемые в результате освоения учебной дисциплины, рассмотрены через соответствующие знания, умения и владения. Для проверки уровня освоения дисциплины предлагаются вопросы к зачету и тестовые материалы, где каждый вариант содержит задания, разработанные в рамках основных тем учебной дисциплины и включающие терминологические задания. Фонд оценочных средств являются составной частью учебно-методического обеспечения процедуры оценки качества освоения образовательной программы и обеспечивает повышение качества образовательного процесса и входит, как приложение, в состав рабочей программы дисциплины. Основные методические указания для обучающихся по дисциплине указаны в разделе основная и дополнительная литература.