МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

Кафедра «Управление и защита информации»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ 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

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.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОПК-2	Способен применять программные средства системного и прикладного назначения для решения профессиональных задач
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-12	Способен участвовать в разработке программно-аппаратных средств защиты информации компьютерных систем и сетей
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

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

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

РАЗДЕЛ 1
Введение

Тема: Основные понятия обратной разработки программной разработки.

РАЗДЕЛ 2
Методики проведения обратной разработки

Тема: 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.

РАЗДЕЛ 3
Средства обратной разработки программной разработки

Тема: Отладчики для реверс-инжиниринга
1) x64dbg
2) WinDbg
3) OllyDbg

РАЗДЕЛ 4
Дизассемблеры для реверс-инжиниринга

Тема: IDA Disassembler
- Radare2

РАЗДЕЛ 5
Вспомогательные утилиты для реверс-инжиниринга

Тема: Detect it Easy (DiE)
ExeInfoPE;
HxD;
HIEW;
Pestudio;
PE-bear;
Fakenet-NG;
ProcessExplorer;
RegShot;
TCPView;
Resource Hacker;

РАЗДЕЛ 6
Средства статического анализа

Тема: Jadx
Apktool;
APKiD;
Simplify;
DeGuard;
Bytecode Viewer;
QARK;
АК-ВС.

РАЗДЕЛ 7
Средства динамического анализа

Тема: Frida
Objection;
Inspeckage;
Drozer;
АК-ВС.