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 - программа специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита программ и данных

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2022

1. Общие сведения о дисциплине (модуле).

Целью дисциплины «Защита программ и данных» является теоретическая и практическая подготовка специалистов к деятельности, связанной с применением современных технологий анализа программных реализаций, защиты программ и программных систем от анализа и вредоносных программных воздействий. Основной целью изучения учебной дисциплины « Защита программ и данных» является формирование у обучающегося компетенций для научно-исследовательского и эксплуатационного видов деятельности. Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видом деятельности): сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности; участие в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах; изучение и обобщение опыта работы других учреждений, организаций и предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте; разработка математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов; установка, наладка, тестирование и обслуживание аппаратно-программных средств обеспечения информационной безопасности компьютерных систем; установка, наладка, тестирование и обслуживание системного и прикладного программного обеспечения; проведение аттестации технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности или профилям защиты.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

ОПК-7 - Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования

для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;

ОПК-14 - Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации;

ПК-1 - Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить научно-исследовательские работы по оценке защищенности информации в компьютерных системах;

ПК-11 - Способен проводить проверки эффективности и выполнять работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации.

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

Уметь:

Использует нормативные правовые акты и нормативные методические документы, регламентирующие деятельность по информационной безопасности, в своей профессиональной деятельности.

Уметь:

Использует нормативные правовые акты и нормативные методические документы, регламентирующие деятельность по разработке и сопровождению современных компьютерных систем, в своей профессиональной деятельности.

Уметь:

Имеет представление о различных методах научных исследований, их выборе и областях применения.

Владеть:

Владеет навыками выбора методов научных исследований при решении конкретных задач.

Уметь:

Умеет ставить и анализировать задачу при проведении разработок в области обеспечения безопасности компьютерных систем и сетей с точки зрения выбранного методы научных исследований.

Владеть:

Владеет навыками по выявлению и дифференциации нарушений работоспособности подсистем защиты информации в операционных

системах, программно-аппаратных средствах защиты информации, в прикладном и системном программном обеспечении.

Знать:

Знает последовательность действий по восстановлению работоспособности подсистем защиты информации в операционных системах, программно-аппаратных средствах защиты информации, в прикладном и системном программном обеспечении; умеет применять на практике эти знания.

Уметь:

Умеет анализировать результаты выполненных работ по восстановлению работоспособности подсистем защиты информации в операционных системах, программно-аппаратных средствах защиты информации, в прикладном и системном программном обеспечении; делать соответствующие выводы и строить свою деятельность в зависимости от достигнутых результатов и полученных выводов.

Уметь:

Участвует в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах.

Уметь:

Изучает и анализирует отечественный и зарубежный опыт по проблемам компьютерной безопасности.

Уметь:

Участвует в проведении экспериментально-исследовательских работ при сертификации средств защиты информации.

Уметь:

Обосновывает критерии и рассчитывает показатели эффективности защиты обрабатываемой информации.

Уметь:

Составляет методики тестирования, подбирает инструментарии? и осуществляет проверку эффективности функционирования программных, программно-аппаратных и технических средств, подсистем защиты информации.

Уметь:

Выполняет работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 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 №9
Контактная работа при проведении учебных занятий (всего):	68	68
В том числе:		
Занятия лекционного типа	34	34
Занятия семинарского типа	34	34

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 76 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	Анализ программных реализаций 1.Задача анализа программных реализаций. Метод экспериментов, статический метод, динамический метод. Принципы функционирования отладчиков. Факторы, ограничивающие возможности отладчиков. 2. Методы поиска функций защиты в машинном коде: метод маяков, метод Step-Trace. 3. Анализ потоков данных. Особенности анализа оверлейного кода, параллельного кода. 4. Особенности анализа машинного кода в среде, управляемой сообщениями.
2	1.Понятие программной закладки. Классификация программных закладок. 2.Модель «наблюдатель»: модульная структура закладки, организация информационного взаимодействия между клиентской и серверной частями. 3. Модель «перехват»: перехватчики паролей первого, второго и третьего рода, защита от перехватчиков паролей первого рода в Windows, средства и методы перехвата сетевого трафика, перехват обращений пользователя к документам, электронной почте и веб-страницам.
3	Защита программ от анализа 1.Защита от дизассемблирования. Защита от отладки. 2. Методы встраивания защиты в программное обеспечение.
4	Внедрение программных закладок 1. Предпосылки к внедрению программных закладок: уязвимости программного обеспечения, уязвимости политики безопасности, человеческий фактор. 2. Методы внедрения программных закладок: маскировка под «безобидное» программное обеспечение, подмена, прямое и косвенное ассоциирование.
5	Противодействие программным закладкам 1. Методы выявления программных закладок: сигнатурное и эвристическое сканирование, контроль целостности, мониторинг информационных потоков, изолированная программная среда, программные ловушки. 2. Принципы построения политики безопасности, обеспечивающей высокую защищенность от программных закладок.
6	Компьютерные вирусы как особый класс программных закладок 1. Бинарные вирусы Windows и Linux: структура, порядок инициализации, алгоритмы поиска и заражения жертвы. 2. Сетевые вирусы: онлайн-вирусы, почтовые вирусы, IM-вирусы. Скриптовые вирусы: макровирусы, shell-вирусы, HTML-вирусы. Комбинированные вирусы. 3. Средства и методы маскировки вирусов и противодействия антивирусному программному обеспечению: стелс-технологии, полиморфные преобразования кода.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	ПЗ 1. Анализ программных реализаций консольных программ
2	ПЗ 2. Текущий контроль по разделу 1 и 2.

№ п/п	Тематика практических занятий/краткое содержание
3	ПЗ 3. Анализ программных реализаций графических программ Windows
4	ПЗ 4. Средства и методы защиты программ от анализа
5	ПЗ 5. Текущий контроль по разделам 3-5.
6	ПЗ 6. Уязвимости программного обеспечения
7	ПЗ 7. Организация антивирусной защиты рабочей станции

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	СР1 Подготовка к практическим занятиям Повторение лекционного материала Изучение тем: Особенности анализа машинного кода в среде, управляемой сообщениями - из учебной литературы из приведенных источников: [1] 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины 5. Конспектирование изученного материала
2	СР2 1. Подготовка к практическим занятиям 2. Повторение лекционного материала 3. Изучение тем: Методы встраивания защиты в программное обеспечение - из учебной литературы из приведенных источников:[1] 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины 5. Конспектирование изученного материала 6. Подготовка к текущему контролю ПК 1
3	СР3 1. Подготовка к практическим занятиям 2. Повторение лекционного материала 3. Изучение тем: Модель «наблюдатель»: модульная структура закладки, организация информационного взаимодействия между клиентской и серверной частями. - из учебной литературы из приведенных источников: [1], доп [1] 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины 5. Конспектирование изученного материала
4	СР4 1. Подготовка к практическим занятиям 2. Повторение лекционного материала 3. Изучение тем: Методы внедрения программных закладок: маскировка под «безобидное» программное обеспечение, подмена, прямое и косвенное ассоциирование - из учебной литературы из приведенных источников:[1], доп [1] 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины 5. Конспектирование изученного материала
5	СР5 1. Подготовка к практическим занятиям 2. Повторение лекционного материала 3. Изучение тем: Методы выявления программных закладок: сигнатурное и эвристическое сканирование, контроль целостности, мониторинг информационных потоков, изолированная программная среда, программные ловушки - из учебной литературы из приведенных источников:[1], доп [1] 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины 5. Конспектирование изученного материала 6. Подготовка к текущему контролю ПК 2
6	СР6 1. Подготовка к практическим занятиям 2. Повторение лекционного материала 3. Изучение тем: Принципы функционирования отладчиков. Факторы, ограничивающие возможности отладчиков -

№ п/п	Вид самостоятельной работы
	из учебной литературы из приведенных источников: [1], доп [1] 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины 5. Конспектирование изученного материала
7	Подготовка к промежуточной аттестации.
8	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства) А.А. Корниенко, М.А. Еремеев, С.Е. Ададуров; Ред. А.А. Корниенко; Под Ред. А.А. Корниенко Однотомное издание Маршрут , 2006	НТБ (ЭЭ); НТБ (уч.3); НТБ (фб.); НТБ (чз.2)
1	Безопасность операционных систем и приложений В.П. Соловьев, Н.В. Павленко, Н.Н. Пуцко; Ред. В.П. Соловьев; МИИТ. Центр компетентности "Защита и безопасность информации" Однотомное издание МИИТ , 2007	НТБ (ЭЭ); НТБ (фб.); НТБ (чз.2)

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

ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ) http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ. http://elibrary.ru/ - научно-электронная библиотека. http://robotosha.ru/ www.chipinfo.ru. http://siblec.ru/ http://autex.ru/ http://www.intuit.ru http://twirpx.com http://habrahabr.ru http://semestr.ru htth://www.cisco.ru Поисковые системы: Yandex, Google, Mail, база научно-технической информации ВИНИТИ РАН. 13. http://www.fstec.ru - сервер ФСТЭК (Федеральная служба по техническому и экспортному контролю 14. http://www.itsec.ru - информационная безопасность 15. http://www.security.lab.ru - информационный портал в области защиты информации 16. http://www.fstec.ru – материалы сайта фирмы «Лаборатория Касперского»

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

Для проведения лекционных занятийнеобходима специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.Для проведения практическихзанятий необходимы компьютеры с рабочими местами в компьютерном классе. Компьютеры должны быть обеспечены лицензионными программными продуктами: Microsoft Office или Work'11, интегрированная среда разработки программного обеспечения для эиуляции сетевого оборудования OmniGraffle; среда разработки программного обеспечения HTML5 и PHP. Для проведения практических занятий и выполнения курсовой работы необходимо иметь комплекс программ для ПЭВМ, обеспечивающих возможность выполнения работ: в области построения программных и аппаратных средств защиты информации в телекоммуникационных сетях (iOS15 Cisco и выше) с поддержкой MPLS; программные продукты Mac OS server, XSan.

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

Для проведения аудиторных занятий и самостоятельной работы требуется:1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET и INTRANET. 2. Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской. 3. Компьютерный класс. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANETДля проведения практических занятий:компьютерный класс; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

9. Форма промежуточной аттестации:

Зачет в 9 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.М. Алексеев

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин