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)

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: 01.06.2025

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 типом задач профессиональности 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:

Знать:

- Нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации (учреждении, предприятии).
- Методологию проведения теоретических и экспериментальных исследований систем защиты информации для оценки защищенности компьютерных систем.
- Принципы организации, архитектуру и состав программных, программно-аппаратных и технических средств, а также подсистем защиты информации.
- Современные языки программирования (высокого и низкого уровня) и инструментальные средства разработки, применяемые для создания защищенного программного обеспечения.
- Требования по защите информации, предъявляемые к проектированию баз данных и администрированию СУБД.

Уметь:

- Участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах.
- Изучать и анализировать отечественный и зарубежный опыт по проблемам компьютерной безопасности.
- Участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации.

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

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

- Применять методы и инструменты программирования для создания и анализа защищенных программных реализаций.

Владеть:

- Навыками составления методики тестирования, подбора инструментария и осуществления проверки эффективности функционирования программных, программно-аппаратных и технических средств, подсистем защиты информации.

- Методами анализа программного кода (статический и динамический анализ) для выявления уязвимостей и закладок.

- Навыками проектирования баз данных с учетом требований информационной безопасности.

- Методами проведения научно-исследовательских работ и оценки защищенности информации в компьютерных системах.

- Инструментальными средствами для восстановления работоспособности 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):	64	64
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	32	32

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 80 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 Рассматриваемые вопросы: - Задача анализа программных реализаций. - Метод экспериментов, статический метод, динамический метод. - Принципы функционирования отладчиков. - Факторы, ограничивающие возможности отладчиков. - Методы поиска функций защиты в машинном коде: метод маяков, метод Step-Trace. - Анализ потоков данных. - Особенности анализа оверлейного кода, параллельного кода. - Особенности анализа машинного кода в среде, управляемой сообщениями.
2	Защита программ от анализа Рассматриваемые вопросы: - Защита от дизассемблирования. - Защита от отладки. - Методы встраивания защиты в программное обеспечение.
3	Программные закладки Рассматриваемые вопросы: - Понятие программной закладки. - Классификация программных закладок. - Модель «наблюдатель»: модульная структура закладки, организация информационного взаимодействия между клиентской и серверной частями. - 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. - Модель «искажение»: применение программных закладок для несанкционированного повышения полномочий пользователя.

№ п/п	Тематика лекционных занятий / краткое содержание
4	Внедрение программных закладок Рассматриваемые вопросы: - Предпосылки к внедрению программных закладок: уязвимости программного обеспечения, уязвимости политики безопасности, человеческий фактор. - Методы внедрения программных закладок: маскировка под «безобидное» программное обеспечение, подмена, прямое и косвенное ассоциирование.
5	Противодействие программным закладкам Рассматриваемые вопросы: - Методы выявления программных закладок: сигнатурное и эвристическое сканирование, контроль целостности, мониторинг информационных потоков, изолированная программная среда, программные ловушки. - Принципы построения политики безопасности, обеспечивающей высокую защищенность от программных закладок.
6	Компьютерные вирусы как особый класс программных закладок Рассматриваемые вопросы: - Бинарные вирусы Windows и Linux: структура, порядок инициализации, алгоритмы поиска и заражения жертвы. - Сетевые вирусы: онлайн-вирусы, почтовые вирусы, IM-вирусы. - Скриптовые вирусы: макровирусы, shell-вирусы, HTML-вирусы. - Комбинированные вирусы. - 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	Анализ программных реализаций консольных программ В результате работы на практическом занятии студент отрабатывает навык анализирования программных реализаций консольных программ с использованием статического и динамического методов. Рассматриваются принципы функционирования отладчиков.
2	Анализ программных реализаций графических программ Windows В результате работы на практическом занятии студент отрабатывает навык анализирования программных реализаций графических программ Windows. Изучаются особенности анализа оверлейного кода и кода в среде, управляемой сообщениями.
3	Методы защиты программ от дизассемблирования и отладки В результате работы на практическом занятии студент рассматривает основные средства и методы защиты программ от анализа, включая защиту от дизассемблирования и отладки. Изучаются методы встраивания защиты в ПО.
4	Анализ уязвимостей программного обеспечения В результате работы на практическом занятии студент изучает типовые уязвимости программного обеспечения (переполнение буфера, форматная строка) и методы их выявления. Рассматриваются предпосылки к внедрению программных закладок.
5	Организация антивирусной защиты рабочей станции В результате работы на практическом занятии студент отрабатывает навык организации антивирусной защиты рабочей станции, включая сигнатурное и эвристическое сканирование, настройку политик безопасности.

№ п/п	Тематика практических занятий/краткое содержание
6	Классификация и анализ программных закладок В результате работы студент изучает модели программных закладок («наблюдатель», «перехват», «искажение»), анализирует методы внедрения и принципы их функционирования.
7	Исследование компьютерных вирусов В результате работы студент рассматривает структуру и алгоритмы функционирования различных классов вирусов (бинарные, сетевые, скриптовые) в ОС Windows и Linux.
8	Методы противодействия программным закладкам В результате работы студент изучает методы выявления программных закладок (контроль целостности, мониторинг потоков, программные ловушки) и принципы построения защищенной политики безопасности.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к практическим занятиям.
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	Криптографические методы защиты информации: классическая криптография Борисова С. Н. Учебное пособие М.: Пензенский государственный университет, - 186 с. - ISBN 978-5-907102-51-4 , 2018	https://reader.lanbook.com/book/162235
2	Управление информационной безопасностью Поздняк И.С. Учебно-методическое издание Самара: ПГУТИ, - 43 с. , 2019	https://reader.lanbook.com/book/223313#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.

Work’11, интегрированная среда разработки программного обеспечения для эиуляции сетевого оборудования OmniGraffle;

среда разработки программного обеспечения HTML5 и PHP.

программные продукты Mac OS server, XSan.

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 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