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 магистратуры
по направлению подготовки
09.04.01 Информатика и вычислительная техника,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Антивирусная защита компьютерных систем

Направление подготовки: 09.04.01 Информатика и вычислительная техника

Направленность (профиль): Компьютерные сети и технологии

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Антивирусная защита компьютерных систем» является формирование компетенций по основным разделам теоретических и практических основ проектирования подсистем антивирусной защиты компьютерных систем.

Основными задачами дисциплины являются:

• Ознакомление с особенностями работы и проектирования современных средств антивирусной защиты.

• Изучение особенностей практического применения средств антивирусной защиты и ее актуализации.

• Изучение технологий обнаружения вирусов в современных системах антивирусной защиты.

• Изучение методов построения решающих правил в современных системах антивирусной защиты.

Дисциплина предназначена для получения знаний, необходимых для решения следующих профессиональных задач (в соответствии с видами деятельности):

Научно-исследовательская деятельность

• Анализ требований к разрабатываемым средствам антивирусной защиты;

• Исследование функциональных и метрологических свойств разрабатываемых средств антивирусной защиты;

• Исследование эффективности и помехоустойчивости разработанных средств антивирусной защиты.

Проектная деятельность

• Сбор и анализ исходных данных для проектирования средств антивирусной защиты;

• Проектирование программных средств антивирусной защиты (систем, программ, баз данных и т.п.) в соответствии с техническим заданием с использованием средств автоматизации проектирования;

• Разработка и оформление проектной и рабочей технической документации;

• Контроль соответствия разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам.

Производственно-технологическая деятельность

• Разработка технологических решений при проектировании современных и перспективных средств антивирусной защиты;

• Разработка технологических решений для оценки надежности и тестирования современных и перспективных средств антивирусной защиты.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-5 - Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем;

ОПК-7 - Способен адаптировать зарубежные комплексы обработки информации и автоматизированного проектирования к нуждам отечественных предприятий;

ПК-3 - Способностью формировать технические задания и участвовать в разработке аппаратных и (или) программных средств вычислительной техники.

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

Знать:

- основные методы и принципы исследований и разработки новых решений при проектировании средств антивирусной защиты компьютерных систем.

Уметь:

- искать и анализировать существующие решения в области разработки средств антивирусной защиты компьютерных систем, адаптировать их для решения задач в новых предметных областях.

Владеть:

- навыками анализа методов решения новых задач в области антивирусной защиты, а также приемами разрешения проблемных ситуаций с помощью адаптации существующих или разработки новых средств антивирусной защиты.

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	Сем. №3
Контактная работа при проведении учебных занятий (всего):	32	32
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	16	16

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	Тема 1. Антивирусная защита. Общие сведения и понятия. Рассматриваемые вопросы: Проблема защиты программ и данных. Информационная и кибербезопасность. Проблема криминализации информационного пространства. Вирусные атаки: потенциальные угрозы и методы защиты. Решение задач антивирусной защиты на мировом уровне. Поиск и анализ актуальной информации о современных методах и средствах антивирусной защиты. Применение перспективных методов исследования и решения профессиональных задач при разработке программ антивирусной защиты в государственных и коммерческих предприятиях России.

№ п/п	Тематика лекционных занятий / краткое содержание
	Тема 2. История компьютерных вирусов от 1983 года до наших дней. Рассматриваемые вопросы: Джон фон Нейман и Фред Коэн. Программа Pervading Animal (1963). 1969: появление первой глобальной сети, вируса и антивируса. 1981: персональные компьютеры и «игровые» вирусы. Elk Cloner. 1984: первые антивирусные программы CHK4BOMB и BOMBSQAD. 1986: первая глобальная эпидемия (вирус Brain). 1988: первая вирусная мистификация. 1988: глобальная эпидемия червя Морриса. 1988: первый антивирусный комплекс: Dr. Solomon's Anti-Virus Toolkit. 1989: первая эпидемия трояна Aids Information Diskette. 1990: Norton AntiVirus. 1995: Concept - первый вирус, поражавший документы Microsoft Word. 1997: Linux.Bliss – первый вирус для Linux. 1999: глобальная эпидемия Melissa - первого вируса для MS Word. 2000: вирус Liberty заражал карманные компьютеры PalmPilot с операционной системой PalmOS. 2001: почтовый червь Sircam. 2003: эпидемия интернет-червя Slammer, заражающего сервера под управлением Microsoft SQL Server 2000. 2004: Bizex (также известный как Exploit) - первый ICQ -червь. Вирусы и тенденции нового времени. Поиск и анализ актуальной информации о современных вирусах и антивирусах. Применение перспективных методов и решений на основе знания мировых тенденций для организации антивирусной защиты предприятия. Тема 3. Вирусы и их классификация. Рассматриваемые вопросы: Вредоносные программы: компьютерные вирусы, черви, трояны и пр. Загрузочные и файловые вирусы. Макровирусы и скрипт-вирусы. Шифрование и метаморфизм. Черви: сетевые, почтовые, IM, IRC, P2P. Трояны: клавиатурные шпионы, похитители паролей, утилиты скрытого удаленного управления, анонимные прокси-сервера, утилиты дозвона, логические бомбы, модификаторы настроек браузера. Условно опасные программы: Riskware, Рекламные утилиты (adware), Pornware, злые шутки. Поиск и анализ актуальной информации о современных методах классификации вирусов. Тема 4. Признаки присутствия на компьютере вредоносных программ. Рассматриваемые вопросы: Общие сведения и виды проявлений: явные, косвенные и скрытые. Изменение настроек браузера. Всплывающие сообщения. Несанкционированное обращение к Интернет. Блокирование антивируса. Блокирование антивирусных сайтов. Сбои в системе или в работе других программ. Почтовые уведомления. Скрытые проявления: наличие в памяти подозрительных процессов; наличие на компьютере подозрительных файлов; наличие подозрительных ключей в системном реестре Windows; подозрительная сетевая активность. Где искать: процессы, автозапуск, системный реестр Windows, конфигурационные файлы, сетевая активность. Поиск и анализ актуальной информации о современных признаках присутствия на компьютере вредоносных программ. Проектирование программ обнаружения признаков присутствия вредоносных программ. Тема 5. Методы защиты от вредоносных программ. Рассматриваемые вопросы: Общие сведения. Организационные методы (правила поведения, политика безопасности). Технические методы (брэндмауэры, средства борьбы со спамом, закладки и пр.). Черные и белые списки адресов. Базы данных образцов спама. Самообучение. Анализ служебных заголовков. Поиск и анализ актуальной информации о современных методах защиты от вредоносных программ. Применение перспективных методов исследования при разработке современных технологий защиты от вредоносных программ. Проектирование методов защиты и их реализация в политиках безопасности. Тема 6. Основы работы антивирусных программ. Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	Сигнатурные методы и эвристические методы. Сигнатурный анализ. Эвристики. Поиск вируса, похожего на известные: вероятность ошибочно определить наличие в файле вируса, невозможность лечения, низкая эффективность. Поиск вируса, выполняющего подозрительные действия: удаление файла, запись в файл, запись в определенные области системного реестра, открытие порта на прослушивание, перехват данных вводимых с клавиатуры, рассылка писем. Проблемы: ложные срабатывания, невозможность лечения, невысокая эффективность. Базовые модули антивирусного ПО: модуль обновления, модуль планирования, модуль управления. Функционал блока управления: Поддержка удаленного управления и настройки, Защита настроек от изменений, карантин. Тестирование работы антивируса. Поиск и анализ актуальной информации о современных антивирусных программах и их использовании. Применение перспективных методов при разработке современных антивирусных программ. Проектирование базовых модулей антивирусного ПО. Тема 7. Антивирусная защита домашнего компьютера. Рассматриваемые вопросы: Антивирусное программное обеспечение. Программы для защиты от несанкционированного доступа и сетевых хакерских атак. Фильтры нежелательной корреспонденции. Проверка в режиме реального времени. Проверка по требованию. Поддержание актуальности антивирусных баз. Фильтрация нежелательных электронных сообщений. Персональная антиспамовая программа. Поиск и анализ актуальной информации о современных антивирусных программах для защиты домашнего компьютера и их использовании. Применение перспективных методов при разработке антивирусных программ. Проектирование антивирусного ПО для защиты домашнего компьютера. Тема 8. Антивирусная защита компьютерной сети и мобильных пользователей. Рассматриваемые вопросы: Основы построения локальной компьютерной сети. Рабочие станции и сетевые серверы, почтовые серверы и шлюзы. Уровни антивирусной защиты: уровень защиты рабочих станций и сетевых серверов, уровень защиты почтовых серверов, уровень защиты шлюзов. Централизованное управление антивирусной защитой. Компоненты системы удаленного централизованного управления: клиентская антивирусная программа, сервер администрирования, агент администрирования, консоль администрирования. Организация сбора статистики в системе антивирусной защиты. Червь Caribe - вредоносная программа для мобильных телефонов. Антивирусы для мобильных устройств. Политики обеспечения информационной безопасности при работе с мобильными устройствами. Политика «нулевого доверия». Поиск и анализ актуальной информации о современных антивирусных программах для защиты компьютерных сетей и их использовании. Применение перспективных методов при разработке антивирусных программ для защиты компьютерных сетей. Проектирование антивирусного ПО для защиты компьютерных сетей.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	1. Признаки присутствия на компьютере вредоносных программ В результате выполнения лабораторной работы студент получает навыки в обнаружении на компьютере различных видов вредоносных программ. 2. Антивирусная защита домашнего компьютера В результате выполнения лабораторной работы студент получает навыки в организации антивирусной

№ п/п	Наименование лабораторных работ / краткое содержание
	защиты домашнего компьютера. 3. Антивирусная защита компьютерной сети и мобильных пользователей В результате выполнения лабораторной работы студент получает навыки в организации антивирусной защиты компьютерной сети.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к лабораторным работам
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	Защита программ и данных. Способы анализа. Ч. 1: учебное пособие. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2020.-72с	https://e.lanbook.com/book/180081(дата обращения: 02.10.2022).- Текст электронный.
2	Защита программ и данных. Способы защиты. Ч. 2: учебное пособие. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2020.-52с	https://e.lanbook.com/book/180082(дата обращения: 02.10.2022).- Текст электронный.
3	Ермакова А.Ю. Методы и средства защиты компьютерной информации: учебное пособие. МИРЭА - Российский технологический университет, 2020.-223с	https://e.lanbook.com/book/163844 (дата обращения: 02.10.2022).- Текст электронный.
4	Пугин В. В., Голубничая Е. Ю., Лабада С. А. Защита информации в компьютерных информационных системах: учебное пособие. Поволжский государственный университет телекоммуникаций и информатики, 2018.-119с	https://e.lanbook.com/book/182299 (дата обращения: 02.10.2022).- Текст электронный.
5	Леонтьев А. С. Защита информации: учебное пособие. МИРЭА - Российский технологический университет 2021.-79с	https://e.lanbook.com/book/182491 (дата обращения: 02.10.2022).- Текст электронный.

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

• Форум специалистов по информационным технологиям http://citforum.ru/

• Интернет-университет информационных технологий http://www.intuit.ru/

• Тематический форум по информационным технологиям http://habrahabr.ru/

• ЭБС "Лань" https://e.lanbook.com/book/

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

• Microsoft Windows

• Microsoft Office

При организации обучения по дисциплине (модулю) с применением электронного обучения и дистанционных образовательных технологий необходим доступ каждого студента к информационным ресурсам – библиотечному фонду Университета, сетевым ресурсам и информационно-телекоммуникационной сети «Интернет».

В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий может понадобиться наличие следующего программного обеспечения (или их аналогов): ОС Windows, Microsoft Office, Интернет-браузер, Microsoft Teams и т.д.

В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта, скайп, Zoom, WhatsApp и т.п.

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

- Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций

Проектор для вывода изображения на экран для студентов, акустическая система, место для преподавателя оснащенное компьютером (CP UCorei3, 8GBRAM, 1Tb HDD, GeForce GTSeries). Аудитория подключена к интернету МИИТ.

- Учебная аудитория для проведения лабораторных работ

персональные компьютеры (процессор intelPentium 2.3 Ghz, 1 Гб оперативной памяти)

- В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации.

Допускается замена оборудования его виртуальными аналогами.

9. Форма промежуточной аттестации:

Зачет в 3 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

доцент, доцент, к.н. кафедры
«Вычислительные системы, сети и
информационная безопасность» С.В. Малинский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А.Клычева