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-2 - Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач;

ОПК-8 - Способен осуществлять эффективное управление разработкой программных средств и проектов.;

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	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

№ п/п	Тематика лекционных занятий / краткое содержание
	разработке программ антивирусной защиты в государственных и коммерческих предприятиях России.
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.
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.
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;

№ п/п	Тематика лекционных занятий / краткое содержание
	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.
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.
6	Основы работы антивирусных программ Рассматриваемые вопросы: -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.
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;

№ п/п	Тематика лекционных занятий / краткое содержание
	-Проектирование антивирусного ПО для защиты домашнего компьютера.
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.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Признаки присутствия на компьютере вредоносных программ В результате выполнения практических заданий студент получает навыки в обнаружении на компьютере различных видов вредоносных программ.
2	Признаки присутствия на компьютере вредоносных программ (продолжение) В результате выполнения практических заданий студент получает навыки в обнаружении на компьютере различных видов вредоносных программ.
3	Антивирусная защита домашнего компьютера В результате выполнения практических заданий студент получает навыки в организации антивирусной защиты домашнего компьютера
4	Антивирусная защита домашнего компьютера (продолжение) В результате выполнения практических заданий студент получает навыки в организации антивирусной защиты домашнего компьютера
5	Антивирусная защита компьютерной сети и мобильных пользователей В результате выполнения практических заданий студент получает навыки в организации антивирусной защиты компьютерной сети.
6	Антивирусная защита компьютерной сети и мобильных пользователей (продолжени В результате выполнения практических заданий студент получает навыки в организации антивирусной защиты компьютерной сети.
7	Сравнительный анализ средств антивирусной защиты компьютерной сети В результате выполнения практических заданий студент получает навыки в сравнительном анализе средств антивирусной защиты компьютерной сети.
8	Сравнительный анализ средств антивирусной защиты компьютерной сети

№ п/п	Тематика практических занятий/краткое содержание
	(продолжение) В результате выполнения практических заданий студент получает навыки в сравнительном анализе средств антивирусной защиты компьютерной сети.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к практическим 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	Диогенес Ю., Озкайя Э. Кибербезопасность. Стратегия атак и обороны. Издательство "ДМК Пресс", 2020 - 326с. – ISBN 978-5-97060-709-1	https://e.lanbook.com/book/131717 (дата обращения: 23.02.2024.- Текст электронный.
2	Никифоров С. Н. Методы защиты информации. Защищенные сети, 2021 - 96с. – ISBN 978-5-8114-7907-8	https://e.lanbook.com/book/167186 (дата обращения: 08.03.2023).- Текст электронный.
3	Мосолов А. С., Акинин Н. И. Компьютерные технологии и методы проектирования в сфере безопасности. Издательство "Лань", 2021 - 444с. – ISBN 978-5-8114-8034-0	https://e.lanbook.com/book/183115 (дата обращения: 23.02.2024).- Текст электронный.
4	Петров А. А. Компьютерная безопасность. Криптографические методы защиты. Издательство "ДМК Пресс", 2008 - 448с. – ISBN 5-89818-064-8	https://e.lanbook.com/book/3027 (дата обращения: 23.02.2024).- Текст электронный.
5	Краковский Ю. М. Методы защиты информации. Издательство "Лань", 2021 - 236с. – ISBN 978-5-8114-5632-1	https://e.lanbook.com/book/156401 (дата обращения: 23.02.2024).- Текст электронный.
6	Тумбинская М.В., Петровский М.В. Защита информации на предприятии: учебное пособие. Издательство "Лань", 2020 - 184с. – ISBN 978-5-8114-4291-1	https://e.lanbook.com/book/130184 (дата обращения: 23.02.2024).- Текст электронный.
7	Прохорова О. В. Информационная безопасность и защита информации. Издательство "Лань", 2022 - 124с. – ISBN 978-5-8114-8924-4	https://e.lanbook.com/book/185333 (дата обращения: 23.02.2024).- Текст электронный.

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/
- Образовательная платформа «Юрайт» https://urait.ru/
- ЭБС ibooks.ru http://ibooks.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. Аудитория подключена к интернету МИИТ.

- Учебная аудитория для проведения лабораторных работ
- персональные компьютеры.
- 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:

Экзамен 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. Андриянова