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 бакалавриата
по направлению подготовки
10.03.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Антивирусная защита

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность 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: 4196
Подписал: заведующий кафедрой Желенков Борис Владимирович
Дата: 23.04.2024

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Антивирусная защита» является формирование компетенций по основным разделам антивирусной защиты вычислительных комплексов, систем и сетей.

Основными задачами дисциплины являются:

• Изучение основ и базовых понятий организации антивирусной защиты вычислительных комплексов, систем и сетей.

• Изучение требований российских и международных стандартов к разработке, внедрению и эксплуатации средств антивирусной защиты вычислительных комплексов, систем и сетей.

• Изучение методов обнаружения вредоносных программ.

• Изучение методов актуализации применяемых антивирусных средств на различных этапах их жизненного цикла.

Д

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-1.1 - Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах;

ПК-3 - способностью администрировать подсистемы информационной безопасности объекта защиты ;

ПК-6 - способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации .

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

Знать:

- основные методы и принципы организации антивирусной защиты вычислительных комплексов, систем и сетей

Уметь:

- применять на практике российские средства антивирусной защиты при обеспечении информационной безопасности вычислительных комплексов, систем и сетей на различных этапах их жизненного цикла

Владеть:

- навыками проведения анализа и оценки эффективности разрабатываемых или действующих средств антивирусной защиты вычислительных комплексов, систем и сетей.

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	Семестр 1
Контактная работа при проведении учебных занятий (всего):	50	50
В том числе:		
Занятия лекционного типа	20	20
Занятия семинарского типа	30	30

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 58 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 компьютерных систем. Общие сведения и терминология Рассматриваемые вопросы: Файлы, файловые системы, программы, вредоносные коды, мобильные носители, компьютерные сети, веб-сайты, гипертекст, электронная почта, почтовый ящик, операционная система, системное и прикладное ПО, уязвимости, патчи, явные и неявные последствия заражения, несанкционированная рассылка, кража конфиденциальной информации, несанкционированное использование сетевых ресурсов, удаленное управление компьютером, ботнеты, атака на компьютер, рассылка спама, фишинг, уничтожение информации, мистификации. Уголовный Кодекс РФ.
2	История компьютерных вирусов с 1983 по 2005 годы. Ситуация и тенденции в 2016-2020 годах Рассматриваемые вопросы: Интернет (1969), Creeper (1971) и Reaper, Elk Cloner (1981), CHK4BOMB (1984), Lehigh (1987) и первая эпидемия, червь Морриса (1988), Anti-Virus Toolkit (1988), Aids Information Diskette (1989) эпидемия троянской программы, Cascade – осыпание букв, Norton AntiVirus (1990), OneHalf (1994)-новая эпидемия, Concept (1995) – вирус для Word, Linux.Bliss (1997) – атака на Linux, Melissa (1999) – новая эпидемия, Liberty (2000) – вирус для карманного компьютера PalmPilot, CodeRed (2001) – новая эпидемия, Slammer (2003) – Интернет-червь, Bizex (2004) – ICQ-червь, Sasser (2004) – червь, поразивший более 8 млн компьютеров, убытки – около 1 млрд USD.
3	Классификации вирусов 3. Тема 3. Классификации вирусов. (2 часа) Рассматриваемые вопросы: Вирусы (загрузочные и файловые), черви (сетевые, почтовые, IM, IRC, P2P), Трояны (клавиатурные шпионы, похитители паролей, утилиты дозвона, анонимные SMTP-сервера и пр.), Adware, Pornware, Злые шутки и пр.
4	Признаки присутствия на компьютере вредоносных программ Рассматриваемые вопросы: Виды проявлений (явные, косвенные и скрытые). Изменение настроек браузера. Всплывающие сообщения. Несанкционированный выход в Интернет. Блокирование антивируса. Блокирование антивирусных сайтов. Сбои в работе системы или в работе других программ.
5	Признаки присутствия на компьютере вредоносных программ (продолжение) Рассматриваемые вопросы: Почтовые уведомления. Где искать? Подозрительные процессы. Автозапуск. Системный реестр Windows. Конфигурационные файлы. Службы Windows.
6	Методы защиты от вредоносных программ Рассматриваемые вопросы: Организационные методы. Технические методы. Политика безопасности и ее разработка. Исправления и автоматические обновления. Брандмауэры (приложение, протокол, адрес, порт, направление, действие. Средства защиты от нежелательной корреспонденции. Черные и белые списки адресов. Самообучение. Анализ служебных заголовков.
7	Основы работы антивирусных программ Рассматриваемые вопросы: Сигнатурный и эвристический методы. Сигнатура вируса и ее анализ. Модули обновления. Модули планирования. Модули управления. Поддержка удаленного управления и настройки. Защита настроек от изменений. Карантин. Тестирование работы антивируса.
8	Классификация антивирусов Рассматриваемые вопросы: Режимы работы антивирусов. Проверка в режиме реального времени. Проверка по требованию. Антивирусные комплексы. Рабочие станции и их защита.
9	Антивирусная защита домашнего компьютера Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	Антивирусное программное обеспечение и его выбор. Проверка в режиме реального времени. Проверка по требованию. Обновление антивирусных баз. Поддержание актуальности антивирусных баз. Защита от несанкционированного доступа и сетевых хакерских атак. Фильтрация нежелательных электронных сообщений.
10	Антивирусная защита компьютерной сети Рассматриваемые вопросы: Основы построения локальной компьютерной сети. Рабочие станции и сетевые сервера. Почтовые сервера. Шлюз. Уровни антивирусной защиты. Централизованное управление антивирусной защитой. Антивирусная защита мобильных пользователей.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Признаки присутствия на компьютере вредоносных программ В результате выполнения лабораторной работы студент получает навыки обнаружения признаков присутствия на компьютере вредоносных программ.
2	Признаки присутствия на компьютере вредоносных программ(продолжение) В результате выполнения лабораторной работы студент получает навыки обнаружения признаков присутствия на компьютере вредоносных программ
3	Основы работы антивирусных программ В результате выполнения лабораторной работы студент получает навыки настройки основных модулей антивирусных программ.
4	. Основы работы антивирусных программ(продолжение) В результате выполнения лабораторной работы студент получает навыки настройки основных модулей антивирусных программ.
5	Антивирусная защита домашнего компьютера В результате выполнения лабораторной работы студент получает навыки установки на домашний компьютер антивирусного ПО и оценки эффективности работы основных модулей установленного ПО.
6	Антивирусная защита домашнего компьютера(продолжение) В результате выполнения лабораторной работы студент получает навыки установки на домашний компьютер антивирусного ПО и оценки эффективности работы основных модулей установленного ПО.
7	Антивирусная защита компьютерной сети В результате выполнения лабораторной работы студент получает навыки установки антивирусного ПО для защиты компьютерной сети.
8	Антивирусная защита компьютерной сети(продолжение) В результате выполнения лабораторной работы студент получает навыки установки антивирусного ПО для защиты компьютерной сети.
9	Комплексный анализ уязвимостей компьютерной сети В результате выполнения лабораторной работы студент получает навыки обнаружения уязвимостей в компьютерной сети.
10	Комплексный анализ уязвимостей компьютерной сети(продолжение) В результате выполнения лабораторной работы студент получает навыки обнаружения уязвимостей в

№ п/п	Наименование лабораторных работ / краткое содержание
	компьютерной сети.
11	Антивирусное ПО и его классификация 11-12. Тема 7. Антивирусное ПО и его классификация(продолжение) В результате выполнения лабораторной работы студент получает навыки сравнительного анализа достоинств и недостатков антивирусного ПО.
12	Антивирусное ПО и его классификация(продолжение) 11-12. Тема 7. Антивирусное ПО и его классификация(продолжение) В результате выполнения лабораторной работы студент получает навыки сравнительного анализа достоинств и недостатков антивирусного ПО.
13	. Антивирусное ПО: сигнатурный и эвристический методы В результате выполнения лабораторной работы студент получает навыки сравнительного анализа достоинств и недостатков сигнатурного и эвристического методов обнаружения вирусных
14	Методы защиты от вредоносных программ В результате выполнения лабораторной работы студент получает навыки в разработке организационных и технических методов защиты от вредоносных программ при реализации политики информационной безопасности предприятия.
15	Методы защиты от вредоносных программ(продолжение) В результате выполнения лабораторной работы студент получает навыки в разработке организационных и технических методов защиты от вредоносных программ при реализации политики информационной безопасности предприятия.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к лабораторным занятиям
3	Подготовка к тестированию
4	Выполнение курсовой работы.
5	Подготовка к промежуточной аттестации.
6	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

Курсовые работы выполняются каждым студентом самостоятельно согласно индивидуальному заданию на тему: «Разработка антивирусной защиты заданной компьютерной системы».

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

№ п/п	Библиографическое описание	Место доступа
1	Монаппа К.А., Анализ вредоносных программ. Издательство «ДМК Пресс», 2019.- 452 с.- ISBN 978-	https://e.lanbook.com/book/123709 (дата обращения: 06.03.2024) -

	5-97060-700-8	Текст электронный.
2	Башлыкова А.А., Проектирование и стандартизация информационных, информационно-вычислительных и телекоммуникационных систем: Учебное пособие. МИРЭА-Российский технологический университет, 2021.- 69с.	https://e.lanbook.com/book/176534 (дата обращения: 06.03.2024) - Текст электронный.
3	Гвоздева Т. В., Баллод Б. А. Проектирование информационных систем. Стандартизация. Издательство "Лань", 2022.-252с.- ISBN 978-5-8114-7963-4	https://e.lanbook.com/book/169810 (дата обращения: 06.03.2024) - Текст электронный.
4	Лагоша О. Н., Сертификация информационных систем. Издательство "Лань" (СПО), 2021- 112с.- ISBN 978-5-8114-7212-3	https://e.lanbook.com/book/156616 (дата обращения: 06.03.2024) - Текст электронный.
5	Семахин А. М., Методы верификации и оценки качества программного обеспечения: Учебное пособие. Курганский государственный университет, 2018- 150с.-ISBN 978-5-4217-0461-4	https://e.lanbook.com/book/177908 (дата обращения: 06.03.2024) - Текст электронный.
6	Миняев А. А., Юркин, Ковцур М. М., Ахрамееева К. А. Сертификация средств защиты информации: учебное пособие. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2020.- 88с.- ISBN 978-5-89160-213-7	https://e.lanbook.com/book/180100 (дата обращения: 06.03.2024) - Текст электронный.
7	Фот Ю. Д., Стандарты информационной безопасности: Учебное пособие. Оренбургский государственный университет, 2018.-226с.- ISBN 978-5-7410-2297-9	https://e.lanbook.com/book/159804 (дата обращения: 06.03.2024) - 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 практических 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:

Курсовая работа в 8 семестре.

Экзамен в 8 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