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)

Защита программ и данных

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: 26.02.2024

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Защита программ и данных» является формирование компетенций по основным разделам теоретических и практических основ проектирования современных систем защиты информации в компьютерных системах. В курсе изучаются методы построения систем антивирусной защиты, а также способы сокрытия информации с использованием криптографических и стеганографических методов.

Основными задачами дисциплины являются:

• Изучение особенностей практического применения методов и средств защиты информации.

• Ознакомление с особенностями работы и проектирования современных средств защиты программ и данных.

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

• Изучение технологий обнаружения вирусов в современных системах антивирусной защиты.

• Изучение способов сокрытия информации криптографическими методами;

• Изучение способов сокрытия информации стеганографическими методами.

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

Эксплуатационная деятельность

• Сбор и анализ данных для изучения и совершенствования систем защиты информации в корпоративных сетях предприятия;

• Сбор и анализ данных для оценки качества функционирования систем защиты информации.

Проектно-технологическая деятельность

• Сбор и анализ данных для проектирования средств информационной защиты корпоративной сети предприятия;

• Проектирование организационных, методических и программных средств информационной 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.

Экспериментально-исследовательская деятельность

• Анализ требований к разрабатываемым методам и средствам защиты программ и данных;

• Исследование функциональных и метрологических свойств разрабатываемых средств защиты программ и данных;

• Исследование эффективности и помехоустойчивости разработанных средств защиты программ и данных.

Организационно-управленческая деятельность

• Разработка организационных методов реализации политики безопасности предприятия при проектировании систем защиты программ и данных;

• Организация и управление коллективной разработкой систем информационной защиты корпоративной сети предприятия.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-1.2 - Способен администрировать средства защиты информации в компьютерных системах и сетях;

ПК-2 - способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач ;

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

ПК-7 - способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений .

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

Знать:

- основные методы и принципы исследований и разработки новых решений при проектировании средств защиты программ и данных в компьютерных сетях предприятия.

Уметь:

-искать и анализировать существующие решения в области разработки средств защиты программ и данных в компьютерных сетях предприятия, адаптировать их для решения задач в новых предметных областях.

Владеть:

- навыками анализа методов решения новых задач в области защиты программ и данных, а также приемами разрешения проблемных ситуаций с помощью адаптации существующих или разработки новых средств информационной 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. №8
Контактная работа при проведении учебных занятий (всего):	52	52
В том числе:		
Занятия лекционного типа	26	26
Занятия семинарского типа	26	26

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 56 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	1 Методы и средства защиты информации. Рассматриваемые вопросы: Классификация методов и средств защиты информации. Методы: препятствие, управление, маскировка, регламентация, принуждение, побуждение. Средства: физические, аппаратные, программные, организационные, законодательные, психологические. Практическое применение методов и средств защиты информации в современных корпоративных сетях. 2 Антивирусная защита. Вирусы и их классификация. Рассматриваемые вопросы: Информационная и кибербезопасность. Проблема криминализации информационного пространства. Вирусные атаки: потенциальные угрозы и методы защиты. Решение задач антивирусной защиты на мировом уровне. 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 и средствах антивирусной защиты. Применение перспективных методов исследования и решения профессиональных задач при разработке программ антивирусной защиты в государственных и коммерческих предприятиях России. 3 Современные методы защиты от вирусов Рассматриваемые вопросы: Методы, основанные на анализе содержимого файлов (как файлов данных, так и файлов с кодами команд). К этой группе относятся сканирование сигнатур вирусов, а также проверка целостности и сканирование подозрительных команд. Методы, основанные на отслеживании поведения программ при их выполнении. Протоколирование всех событий, угрожающих безопасности системы и происходящих либо при реальном выполнении проверяемого кода, либо при его программной эмуляции. Методы регламентации порядка работы с файлами и программами. Наиболее популярные антивирусные программы и их особенности. McAfee, Norton, Panda, Avira, Bitdefender, Bullguard, Heimdal. Антивирус Касперского. Поиск и анализ актуальной информации о применении наиболее популярных антивирусных программ в современных корпоративных системах киберзащиты. 4 Антивирусная защита компьютерной сети и мобильных пользователей Рассматриваемые вопросы: Корпоративные 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

№ п/п	Тематика лекционных занятий / краткое содержание
	программа, сервер администрирования, агент администрирования, консоль администрирования. Организация сбора статистики в системе антивирусной защиты. 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. Проектирование антивирусного ПО для защиты компьютерных сетей. 5 Криптография и ее применение при защите данных в корпоративной сети предприятия. Рассматриваемые вопросы: Криптография: определение, история, применение в современных задачах сокрытия информации. Терминология и ГОСТы: открытый (исходный) текст, шифротекст, ключ, шифрование, асимметричный шифр, открытый ключ, закрытый ключ, криптоанализ. Криптографические методы и алгоритмы. Симметричные и асимметричные алгоритмы. Хеш-функции. Практическое применение криптографии в задачах защиты информации. Поиск и анализ актуальной информации о современных методах и средствах криптографической защиты. Применение перспективных методов и средств криптографии при разработке систем защиты информации. 6 Стеганография и ее применение при защите данных в корпоративной сети предприятия. Рассматриваемые вопросы: Стеганография: определение, история, применение в современных задачах сокрытия информации. Стеганосистема и ее элементы. Потоковый и фиксированный контейнеры. Стегоключ и стегоканал. Сокрытие информации в фото- , видео- и аудиофайлах. Практическое применение стеганографии. Совместное применение криптографических и стеганографических методов в задачах защиты данных. Поиск и анализ актуальной информации о современных методах и средствах стеганографической защиты. Применение перспективных методов и средств стеганографии при разработке систем защиты информации. 7 Требования о защите информации, не составляющей государственную тайну (приказ ФСТЭК №17 от 11.02.2013). Рассматриваемые вопросы: Требования к организации защиты информации, содержащейся в информационной системе. Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы. Три класса защищенности информационной системы. Разработка системы защиты информации информационной системы. Разработка организационно-распорядительных документов по защите информации. Аттестация информационной системы и ввод ее в действие. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	1 Признаки присутствия на компьютере вредоносных программ В результате выполнения практического задания студент получает навыки в обнаружении на компьютере различных видов вредоносных программ. 2 Антивирусная защита компьютерной сети и мобильных пользователей.

№ п/п	Тематика практических занятий/краткое содержание
	В результате выполнения практического задания студент получает навыки в организации антивирусной защиты компьютерной сети. 3 Криптография. Сокрытие информации криптографическими методами В результате выполнения практического задания студент получает навыки в сокрытии информации с помощью различных криптографических алгоритмов. 4 Стеганография. Сокрытие информации в фотофайле. В результате выполнения практического задания студент получает навыки в сокрытии информации стеганографическими методами в массиве фотофайлов. 5 Стеганография. Сокрытие информации в видео- и аудиофайлах. В результате выполнения практического задания студент получает навыки в сокрытии информации стеганографическими методами в видео- и аудиофайлах.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка к практическим занятиям
2	Работа с лекционным материалом
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: 25.02.2024).- Текст электронный.
2	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: 25.02.2024).- Текст электронный.
3	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: 25.02.2024).- Текст электронный.
4	Краковский Ю. М. Методы защиты информации. Издательство "Лань", 2021 - 236с. – ISBN 978-5-8114-5632-1	https://e.lanbook.com/book/156401 (дата обращения: 25.02.2024.- Текст электронный.
5	Тумбинская М.В., Петровский М.В. Защита	https://e.lanbook.com/book/130184

	информации на предприятии: учебное пособие. Издательство "Лань", 2020 - 184с. – ISBN 978-5-8114-4291-1	(дата обращения: 25.02.2024).- Текст электронный.
6	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: 25.02.2024).- Текст электронный.
7	Никифоров С. Н. Методы защиты информации. Защищенные сети, 2021 - 96с. – ISBN 978-5-8114-7907-8	https://e.lanbook.com/book/167186 (дата обращения: 25.02.2024).- Текст электронный.
8	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: 25.02.2024).- Текст электронный.
9	Леонтьев А. С. Защита информации: учебное пособие. МИРЭА - Российский технологический университет 2021.-79с	https://e.lanbook.com/book/18249 (дата обращения: 25.02.2024).- 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 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