МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УВР
_____ А.Г. Жуковский
«_29_» _____08_____ 2022 г.

Защита информации от вредоносного программного обеспечения Б1.В.07
рабочая программа дисциплины

Кафедра: Информатика и вычислительная техника
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем.**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения), курсам (для заочной формы обучения)

Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/6сем		
Контактная работа, в том числе (по семестрам, курсам):		72/6сем		
Лекции		24/6сем		
Лабораторных работ		24/6сем		
Практических занятий		24/6сем		
Семинаров				
Самостоятельная работа		72/6сем		
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с оценкой с разбивкой по семестрам (курсам)				
Число экзаменов с разбивкой по семестрам (курсам)		1/6сем		

Программу составил:
Доцент кафедры ИВТ, к.т.н., с.н.с. Ткачук Е.О.

Рецензент:
Ведущий сотрудник ФГУП «РНИИРС, д.т.н., доцент Елисеев А.В.

Рабочая программа дисциплины
«Защита информации от вредоносного программного обеспечения»

разработана в соответствии с ФГОС ВО:
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020г. N 1427.

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 25.04.2022, и утвержденного директором СКФ МТУСИ 25.04.2022 г.

Рассмотрена и одобрена на заседании кафедры
«Информатика и вычислительная техника»

Протокол от «29» 08 2022г. № 1

Зав. кафедрой _____ С.В. Соколов

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

«Информатика и вычислительная техника»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Информатика и вычислительная техника»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Информатика и вычислительная техника»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Информатика и вычислительная техника»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

1. Цели изучения дисциплины

Целями дисциплины являются формирование у студентов знаний и умений в области защиты информации от вредоносного программного обеспечения (ПО).

Задачи дисциплины состоят в следующем:

- сформировать у студентов знания о целях создания вредоносного программного обеспечения, его основных видах, способах его проникновения в систему и технологиях защиты;
- сформировать у студентов знания о программных уязвимостях, их устранении, а также о технологиях уменьшения риска их эксплуатации;
- обеспечить приобретение навыков реализации технологии обнаружения вредоносного программного обеспечения.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с ***эксплуатационным*** видом деятельности:

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ПК-3: Администрирование средств защиты информации прикладного и системного программного обеспечения
Знать:
- методы ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования
Уметь:
- осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения
Владеть:
- навыками по обнаружению вредоносного программного обеспечения и ликвидации последствий его функционирования - навыками установки, конфигурации и эксплуатации программного обеспечения по защите информации

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Дисциплина «Защита информации от вредоносного программного обеспечения» является логическим продолжением дисциплины Б1.О.11 «Основы информационной безопасности»», знание которой в объеме требований образовательной программы является необходимым.
2	Успешное освоение дисциплины «Защита информации от вредоносного программного обеспечения» базируется также на знаниях, приобретенных из дисциплин: Б1.О.06 «Физика», Б1.О.07 «Иностранный язык», Б1.О.12 «Введение в информационные технологии».
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Дисциплина является базовой для успешного освоения дисциплины Б1.О.39 Методы

	оценки безопасности компьютерных систем (Аудит компьютерных систем)

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 144 часов, 72 аудиторных часов, 72 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 1, Семестр 2					
Модуль 1. Вредоносное программное обеспечение. (Лекции 16 ПЗ 16 СРС 36; 32+36=68) часов					
1.1	Лекция 1. Вредоносное программное обеспечение: история, цели создания, условия существования, способы проникновения в систему.	Л1.	4	ПК-3	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. Классификация объектов, детектируемых антивирусным программным обеспечением.	Л2.	4	ПК-3	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. Спам.	Л3.	4	ПК-3	Л1.1 Л1.2 Л1.3
1.4	Лекция 4 Фишинг	Л4	4	ПК-3	Л1.1 Л1.2 Л1.3
1.5	Практическое занятие №1 Изучение структуры PE-файлов	ПЗ 1	4	ПК-3	Л1.1 Л1.2 Л1.3
1.6	Практическое занятие №2 Способы внедрения вредоносного кода	ПЗ 2	4	ПК-3	Л1.1 Л1.2 Л1.3
1.7	Практическое занятие №3 Дизассемблирование	ПЗ 3	4	ПК-3	Л1.1 Л1.2 Л1.3
1.8	Практическое занятие №4 Отладка	ПЗ 4	4	ПК-3	Л1.1 Л1.2 Л1.3
1.9	Самостоятельная работа 1. Цели создания вредоносного программного обеспечения 2. Условия существования вредоносного программного обеспечения 3. Способы проникновения вредоносного программного обеспечения в систему 4. Классификация детектируемых антивирусным ПО объектов. Вредоносные программы. Вирусы. 5. Классификация детектируемых антивирусным ПО	СРС	36	ПК-3	Л1.1 Л1.2 Л1.3

	объектов. Вредоносные программы. Черви. 6. Классификация детектируемых антивирусным ПО объектов. Вредоносные программы. Троянские программы. Backdoor. 7. Классификация детектируемых антивирусным ПО объектов. Вредоносные программы. Троянские программы. Exploit. 8. Классификация детектируемых антивирусным ПО объектов. Вредоносные программы. Троянские программы. Rootkit. 9. Классификация детектируемых антивирусным ПО объектов. Вредоносные программы. Троянские программы. Trojan-ArcBomb.				
Модуль 2 Основы защиты информации в инфокоммуникационных системах и сетях (Лекции 8 ПЗ 8 ЛР 24 СРС 36; 40+36=76)					
2.1	Лекция №5 Модель системы защиты от вредоносных программ	Л5	4	ПК-3	Л1.1 Л1.2 Л1.3
2.2	Лекция №6 Методы и технологии защиты от вредоносного программного обеспечения	Л6	4	ПК-3	Л1.1 Л1.2 Л1.3
2.3	Практическое занятие №5 Проектирование архитектуры антивирусного программного обеспечения	ПЗ 5	4	ПК-3	Л1.1 Л1.2 Л1.3
2.4	Практическое занятие №6 Создание службы и ее запуск	ПЗ 6	4	ПК-3	Л1.1 Л1.2 Л1.3
2.5	Лабораторная работа №1 Разработка компонента меж процессного взаимодействия	ЛР1	2	ПК-3	Л1.1 Л1.2 Л1.3
2.6	Лабораторная работа №2 Разработка компонента антивирусных баз	ЛР2	2	ПК-3	Л1.1 Л1.2 Л1.3
2.7	Лабораторная работа №3 Разработка компонента сигнатурного сканирования	ЛР3	2	ПК-3	Л1.1 Л1.2 Л1.3
2.8	Лабораторная работа №4 Разработка компонента обнаружения и подготовки к сканированию исполняемых файлов	ЛР4	2	ПК-3	Л1.1 Л1.2 Л1.3
2.9	Лабораторная работа №5 Разработка компонента обнаружения и подготовки к сканированию архивов	ЛР5	2	ПК-3	Л1.1 Л1.2 Л1.3
	Лабораторная работа №6 Разработка компонента сканирования файлов и директорий по запросу	ЛР6	2	ПК-3	Л1.1 Л1.2 Л1.3

	Лабораторная работа №7 Разработка компонента сканирования файлов и директорий по расписанию	ЛР7	2	ПК-3	Л1.1 Л1.2 Л1.3
	Лабораторная работа №8 Разработка компонента мониторинга директорий	ЛР8	2	ПК-3	Л1.1 Л1.2 Л1.3
	Лабораторная работа №9 Разработка компонента «Карантин»	ЛР9	2	ПК-3	Л1.1 Л1.2 Л1.3
	Лабораторная работа №10 Разработка компонента персистентного хранения настроек	ЛР10	2	ПК-3	Л1.1 Л1.2 Л1.3
	Лабораторная работа №11 Разработка компонента персистентного хранения отчетов о сканировании	ЛР11	2	ПК-3	Л1.1 Л1.2 Л1.3
	Лабораторная работа №12 Создание графического пользовательского интерфейса	ЛР12	2	ПК-3	Л1.1 Л1.2 Л1.3
	Самостоятельная работа 1. Модель системы защиты от вредоносных программ. Технический компонент. Работа с файлом как с массивом байтов. 2. Модель системы защиты от вредоносных программ. Технический компонент. Эмуляция кода программы. 3. Модель системы защиты от вредоносных программ. Технический компонент. Запуск программы в «песочнице». 4. Модель системы защиты от вредоносных программ. Технический компонент. Мониторинг системных событий. 5. Модель системы защиты от вредоносных программ. Технический компонент. Поиск системных аномалий. 6. Модель системы защиты от вредоносных программ. Аналитический компонент. Простое сравнение. 7. Модель системы защиты от вредоносных программ. Аналитический компонент. Сложное сравнение. 8. Модель системы защиты от вредоносных программ. Аналитический компонент. Экспертная система. 9. Методы и технологии защиты от вредоносного программного обеспечения.	СРС	36	ПК-3	Л1.1 Л1.2 Л1.3
	Экзамен			ПК-3	Л1.1 Л1.2 Л1.3
Итого – 144 часов					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л1.1	Фаронов А.Е.	Основы информационной безопасности при работе на компьютере	М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020.— 154 с	Э1
Л1.2	Галатенко, В. А.	Основы информационной безопасности :	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с.	Э2
Л1.3	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2	Э3
5.1.2. Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1	М. М. Вулф, Н. Т. Разумовский, Р. Г. Прокди. .	Как защитить компьютер от вирусов	Санкт-Петербург : Наука и Техника, 2010. — 192 с.	Э4
5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л3.1	Гошко, С. В.	Технологии борьбы с компьютерными вирусами : практическое пособие	Москва : СОЛОН-ПРЕСС, 2016. — 351 с.	Э5

5.2. Электронные образовательные ресурсы	
Э1	https://www.iprbookshop.ru/89453.html
Э2	https://www.iprbookshop.ru/97562.html
Э3	https://www.iprbookshop.ru/87995.html
Э4	https://www.iprbookshop.ru/35399.html
Э5	https://www.iprbookshop.ru/90288.html

5.3. Программное обеспечение		
П.1	1. AVAST Free Antivirus 2. AVG AntiVirus Free 3. Dr.Web Antivirus 4. Антивирус Касперского 5. ESET NOD32 Антивирус 6. AVZ Antivirus 7. Avira Free Antivirus 8. Norton AntiVirus	Антивирусное ПО. Свободное, условно свободное или триал-версии.

	9. McAfee Antivirus 10. Emsisoft Anti-Malware 11. BullGuard Antivirus 12. Protector Plus Antivirus 13. Panda Antivirus 14. Ashampoo Anti-Virus 14. G Data AntiVirus 16. K7 AntiVirus 17. VIRUSfighter 18. Twister Antivirus	
П.2	1. Wise Folder Hider 2. Secure Folders 3. Anvide Lock Folder 4. Folder Lock 5. Easy File Locker 6. Folder Guard 7. DEKSI USB Security 8. Locker (защита папок и дисков) 9. Advanced Hider 10. Hide Folders XP 11. Hide Files	Программное обеспечение по защите и сокрытию файлов и папок. Свободное, условно свободное или триал-версии.
П.3	1. TrustPort Tools 2. Cryptic Disk 3. Locker (скрытие файлов) 4. Max File Encryption 5. Secure Disk 6. Masker 7.1 7. Fox Secret 8. HideInPicture 1.0 9. Шифровальщик 10. Advanced Encryption Package 11. Gpg4win 12. Cryptic Disk Professional 13. CyberSafe Files Encryption 14. Steganos Privacy Suite 15. Lavasoft Privacy Toolbox 16. pkiImage Free Edition	Программное обеспечение по шифрованию, безвозвратному удалению, стеганографии. Свободное, условно свободное или триал-версии.
П.4	1. Hetman Partition Recovery 2. Active File Recovery 3. R-Studio 7.6 4. Auslogics File Recovery 5. Active UNDELETE 6. Paragon Rescue Kit 7. Wise Data Recovery 8. Puran File Recovery 9. O&O DiskRecovery 10. Tenorshare Any Data Recovery	Программное обеспечение по восстановлению данных. Свободное, условно свободное или триал-версии.

	11. Power Data Recovery	
	12. GetDataBack	
	13. Recover My Files	
	14. R-Undelete	
	15. Handy Recovery	
	16. Ashampoo Undeleter	
П.5	1. Iperius Backup 2. FBackup 3. Backup4all 4. Uranium Backup Free 5. Simple Data Backup 6. Personal Backup 7. Back4Sure 8. SyncBackFree 9. Handy Backup 10. EASEUS Todo Backup 8.0 Free Edition 11. Exiland Backup Free 4.0 12. Nero BackItUp 13. Paragon Rescue Kit 14.0 Free 14. Action Backup 15. LimBackup 16. AVSbackup 17. ExtraBackup 18. Cobian Backup 19. Backup & Recovery 10 Build 9169 Free Edition 20. Information Backup System	Программное обеспечение по резервному копированию данных. Свободное, условно свободное или триал-версии.
П.6	MS Word – с лицензией	
П.7	Power Point – с лицензией	

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО лабораторных работ и практических занятий	
1	Компьютерная аудитория с выходом в интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерная аудитория

7. Методические указания для обучающихся по освоению дисциплины

7.1 Указания по самостоятельной работе студента

Достижение целей эффективной подготовки студентов в вузах невозможно без их целеустремленной самостоятельной работы. При этом, безусловно, нельзя обойтись без живого общения и консультирования со стороны профессорско-преподавательского состава Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов

(систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам. Обязательным компонентом самостоятельной работы студентов является внеаудиторный практикум по иностранному языку.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов, выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий. учебно-методических материалов, образцов техники
- содержать материал. углубляющий знания, полученные на лекции;
- осваивать проблемные еще не полностью решенные вопросы.

Проведению самостоятельной работы (как и любого другого вида занятий) должна предшествовать подготовка как преподавателя, так и обучаемых.

Постановку задачи обучаемым на проведение самостоятельного занятия преподаватель осуществляет на одном из занятия, предшествующему данному. Он разъясняет смысл занятия и указывает, что к нему студенты должны приготовить. Задание на самостоятельную работу должно быть выдано заблаговременно с тем, чтобы слушатели имели время на информационный поиск в библиотеке необходимых пособий.

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений, техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их обсуждение; работу студентов по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

При возникновении затруднений у обучаемых в разрешении вопросов задания преподавателю необходимо предусмотреть, чтобы каждый обучаемый мог получить оперативную консультацию по любому вопросу, если же при самостоятельной работе возникают затруднения по одному и тому же материалу (вопросу) у многих обучаемых, то желательно провести групповую консультацию.

Для контроля усвоения учебного материала целесообразно проводить в групповое собеседование или обсуждение изучаемого материала, проведение контрольных работ и т.п. Контрольные мероприятия при должной их организации позволяют не только оценивать знания материала, но и углубить и закрепить его у обучаемых.

Приветствуется использование компьютеров, которое:

- расширяет информационную баз) учебных занятий;
- повышает активность обучаемых, из пассивного получателя информации они превращаются в её добытчиков:
- способствует развитию способностей к анализу и обобщению, улучшает связанность, широту и глубину мышления;
- облегчает усвоение абстрактного материала, позволяет многое из него представить в виде конкретных образов;
- приучает к точности, аккуратности, последовательности действий способствует развитию самостоятельности.

Компьютерные технологии и программные продукты для выполнения самостоятельной

работы по освоению учебного материала необходимо использовать в соответствии с указаниями методических разработок раздела 5 настоящей Рабочей программы.

Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта http://www.intuit.ru/ .

Таблица 7.1 – Учебный материал, выносимый на самостоятельное изучение студентам очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 72	Неделя
Модуль 1 – 36 часов			
1	Цели создания вредоносного программного обеспечения	4	1
2	Условия существования вредоносного программного обеспечения	4	2
3	Способы проникновения вредоносного программного обеспечения в систему	4	3
4	Классификация детектируемых антивирусным ПО объектов. Вредоносные программы. Вирусы.	4	4
5	Классификация детектируемых антивирусным ПО объектов. Вредоносные программы. Черви.	4	5
6	Классификация детектируемых антивирусным ПО объектов. Вредоносные программы. Троянские программы. Backdoor.	4	6
7	Классификация детектируемых антивирусным ПО объектов. Вредоносные программы. Троянские программы. Exploit.	4	7
8	Классификация детектируемых антивирусным ПО объектов. Вредоносные программы. Троянские программы. Rootkit. Троянские программы. Trojan-ArcBomb	8	8
Модуль 2 – 36 часов			
9	Модель системы защиты от вредоносных программ. Технический компонент. Работа с файлом как с массивом байтов.	4	9
10	Модель системы защиты от вредоносных программ. Технический компонент. Эмуляция кода программы.	4	10
11	Модель системы защиты от вредоносных программ. Технический компонент. Запуск программы в «песочнице».	4	11
12	Модель системы защиты от вредоносных программ. Технический компонент. Мониторинг системных событий.	4	12
13	Модель системы защиты от вредоносных программ. Технический компонент. Поиск системных аномалий.	4	13
14	Модель системы защиты от вредоносных программ. Аналитический компонент. Простое сравнение.	4	14
15	Модель системы защиты от вредоносных программ. Аналитический компонент. Сложное сравнение.	4	15
16	Модель системы защиты от вредоносных программ. Аналитический компонент. Экспертная система. Методы и технологии защиты от вредоносного программного обеспечения	8	16

Дополнения и изменения в рабочей программе