

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 УР
Н.А. Андреева
« 28 » _____ 2026 г.

Рабочая программа дисциплины

**Б1.В.03 Защита информации от вредоносного
программного обеспечения**

Кафедра	Информационной безопасности
Направление подготовки	10.03.01 Информационная безопасность
Профиль	Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)
Формы обучения	очная

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))

Вид учебной работы	ОФО	
	ЗЕ	часов/семестр
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/6
Контактная работа, в том числе (по семестрам, курсам):		64/6
Лекции		16/6
Лабораторных работ		32/6
Практических занятий		16/6
Семинаров		
Самостоятельная работа		44/6
Контроль		36/6
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам		
Число экзаменов с разбивкой по семестрам		1/6

Программу составил:
К.т.н., доцент Маршаков Д.В.

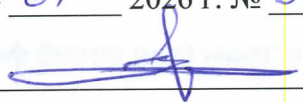
Рабочая программа дисциплины
«Защита информации от вредоносного программного обеспечения»

Разработана в соответствии с **ФГОС ВО**
направление подготовки **10.03.01 Информационная безопасность,**
утвержденное приказом Министерства науки и высшего образования Российской
Федерации от 17 ноября 2020 г. № 1427.

Составлена на основании учебного плана
направления **10.03.01 Информационная безопасность** профиль **Безопасность компьютерных**
систем (по отрасли или в сфере профессиональной деятельности), одобренного Учёным
советом СКФ МТУСИ, протокол № 8 от 31.03. 2026г, и утвержденного
директором СКФ МТУСИ 31.03 2026 г.

Рассмотрена и одобрена на заседании кафедры
"Информационной безопасности "

Протокол от «28» 04 2026 г. № 9.

И.О. Зав. кафедрой  Жуковский А.Г.

1. Цели изучения дисциплины

Целями освоения дисциплины «Защита информации от вредоносного программного обеспечения» является получение обучающимися знаний, формирование у них умений и навыков в области защиты информации от вредоносного программного обеспечения (ПО).

Задачи дисциплины состоят в следующем:

- сформировать у обучающихся знания о целях создания вредоносного программного обеспечения, его основных видах, способах его проникновения в систему и технологиях защиты;
- сформировать у обучающихся 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 обучающегося способности решать профессиональные задачи в соответствии с эксплуатационным видом деятельности. Результатом освоения дисциплины являются сформированные у обучающегося компетенции:

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	Б1.О.05	Введение в информационные технологии
2	Б1.О.14	Информационные технологии и программирование
3	Б1.О.28	Организационное и правовое обеспечение информационной безопасности
4	Б1.В.06	Введение в профессию
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:		
1	Б1.О.29	Методы и средства криптографической защиты информации
2	Б1.О.33	Программно-аппаратные средства защиты информации
3	Б1.О.31	Защита информации от утечки по техническим каналам
4	Б1.В.02	Комплексное обеспечение защиты информации объекта информатизации
5	Б1.О.36.03	Безопасность компьютерных сетей
6	Б1.О.36.06	Администрирование средств защиты информации в компьютерных системах и сетях

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. час.	Комп - тенци и	УМИ О
1	2	3	4	5	6
Курс 3, Семестр 6 – 64 часа аудиторных занятий + 44 часа СРС + контроль 36 ч. = 144 часа					
Модуль 1. Вредоносное программное обеспечение (24 + 22 = 46 часов)					
1.1	Лекция 1. Вредоносное программное обеспечение (ПО): история, цели создания, условия существования, способы проникновения в систему	Лек.	2	ПК-3	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3
1.2	Лекция 2. Классификация объектов, детектируемых антивирусным программным обеспечением	Лек.	2	ПК-3	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3
1.3	Лекция 3. Спам. История, виды, способы распространения. Борьба со спамом. Наиболее распространенные виды спама.	Лек.	2	ПК-3	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3
1.4	Лекция 4 Фишинг данных, навязывание товаров/услуг. Распространенные методики фишинга данных и возможные средства противодействия им.	Лек.	2	ПК-3	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3
1.5	Практическое занятие №1 Изучение структуры PE-файлов	ПЗ	4	ПК-3	Л1.1, Л3.2
1.6	Практическое занятие №2 Способы внедрения вредоносного кода	ПЗ	4	ПК-3	Л1.1, Л3.2,
1.7	Практическое занятие №3 Дизассемблирование	ПЗ	4	ПК-3	Л1.1, Л3.2,
1.8	Практическое занятие №4 Отладка	ПЗ	4	ПК-3	Л1.1, Л3.2,
1.9	1. Цели создания вредоносного ПО 2. Условия существования вредоносного ПО 3. Способы проникновения вредоносного программного обеспечения в систему 4. Классификация детектируемых антивирусным ПО объектов. Вредоносные программы. Вирусы. 5. Классификация детектируемых антивирусным ПО 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	СРС	22	ПК-3	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3

	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 – (40 + 22 = 60 часов)					
2.1	Лекция №5 Модель системы защиты от вредоносных программ	Лек.	4	ПК-3	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3
2.2	Лекция №6 Методы и технологии защиты от вредоносного программного обеспечения	Лек.	4	ПК-3	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3
2.3	Лабораторная работа №1 Разработка компонента меж процессного взаимодействия	ЛР	4	ПК-3	Л1.1, Л2.1 Л3.1
2.4	Лабораторная работа №2 Разработка компонента антивирусных баз	ЛР	2	ПК-3	Л1.1, Л2.1 Л3.1
2.5	Лабораторная работа №3 Разработка компонента сигнатурного сканирования	ЛР	2	ПК-3	Л1.1, Л3.1
2.6	Лабораторная работа №4 Разработка компонента обнаружения и подготовки к сканированию исполняемых файлов	ЛР	2	ПК-3	Л1.1, Л3.1
2.7	Лабораторная работа №5 Разработка компонента обнаружения и подготовки к сканированию архивов	ЛР	2	ПК-3	Л1.1, Л3.1
2.8	Лабораторная работа №6 Разработка компонента сканирования файлов и директорий по запросу	ЛР	4	ПК-3	Л1.1, Л3.1
2.9	Лабораторная работа №7 Разработка компонента сканирования файлов и директорий по расписанию	ЛР	2	ПК-3	Л1.1, Л2.1 Л3.1
2.10	Лабораторная работа №8 Разработка компонента мониторинга директорий	ЛР	2	ПК-3	Л1.1, Л3.1
2.11	Лабораторная работа №9 Разработка компонента «Карантин»	ЛР	2	ПК-3	Л1.1, Л3.1
2.12	Лабораторная работа №10 Разработка компонента персистентного хранения настроек	ЛР	2	ПК-3	Л1.1, Л3.1
2.13	Лабораторная работа №11 Разработка компонента персистентного хранения отчетов о сканировании	ЛР	2	ПК-3	Л1.1, Л3.1
2.14	Лабораторная работа №12 Создание графического пользовательского интерфейса	ЛР	6	ПК-3	Л1.1, Л3.1
2.15	1. Модель системы защиты от вредоносных программ. Технический компонент. Работа с файлом как с массивом байтов.	СРС	22	ПК-3	Л1.1, Л1.2, Л2.1

	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.				Л2.2 Л2.3
	Экзамен		36	ПК-3	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3 Л3.1 Л3.2
	Итого		144		

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	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2024.	Э1
Л1.2	Трофимова, И. П., Ю. А. Сосулин	Хранение и защита информации : учебное пособие	Рязань : Рязанский государственный радиотехнический университет, 2013. — 52 с.	Э2
5.1.2 Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Бубнов А.А., В. В. Тишкина	Тестирование программного обеспечения : учебное пособие	Рязань: Рязанский государственный радиотехнический университет, 2024. — 164 с.	Э3
Л2.2	Александрова, Е. Б.	Криптографические методы защиты информации. Элементы алгебраической геометрии :	Санкт-Петербург: Санкт-Петербургский	Э4

		учебное пособие	политехнический университет Петра Великого, 2023. — 106 с.	
Л2.3	Белоус, А. И., В. А. Солодуха	Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения	Москва: Техносфера, 2021. — 482 с.	Э5

5.1.3 Методическое обеспечение

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Осин А.В., Большаков А.С.	Безопасность приложений. Защита информации от вредоносного программного обеспечения: Учебно-методическое пособие	Москва: МТУСИ, 2022 – 37 с.	Э7
Л3.2	Ларионова, Е. И., Ю. Д. Фот, К. Р. Джукашев	Криптографическая защита информации : практикум	Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2025. — 110 с.	Э8

5.2 Электронные образовательные ресурсы

Э1	https://www.iprbookshop.ru/145912.html
Э2	https://www.iprbookshop.ru/121431.html
Э3	https://www.iprbookshop.ru/150311.html
Э4	https://www.iprbookshop.ru/143094.html
Э5	https://www.iprbookshop.ru/108023.html
Э6	https://elib.mtuci.ru/view.php?book_id=3066
Э7	https://www.iprbookshop.ru/153198.html

5.3 Информационно-справочные системы и профессиональные базы данных

5.3.1	Консультант Плюс – https://www.consultant.ru/
5.3.2	Гарант – https://www.garant.ru/
5.3.2	Консорциум Кодекс – https://docs.cntd.ru/
5.3.3	Научная электронная библиотека – https://www.elibrary.ru/
5.3.4	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)
5.3.5	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)

5.4 Программное обеспечение

СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

П.1	Антивирус Касперского
П.2	Wise Folder Hider
П.3	Cryptic Disk Professional
П.4	Auslogics File Recovery
П.5	SyncBackFree
П.6	OpenOffice Writer
П.7	OpenOffice Impress
П.8	Операционная система Linux

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная проектором, ПК (ноутбуком), экраном
6.2 МТО лабораторных работ и практических занятий	
1	Лаборатория «Программно-аппаратные средства защиты информации», укомплектованная специализированной мебелью, оснащенную программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации»
2	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
6.3 МТО рубежных контролей, зачетов, экзаменов	
1	Учебные аудитории, оборудованные компьютерной техникой с возможностью выхода в локальную сеть Филиала и Интернет.
6.4 МТО самостоятельной работы обучающихся	
1	Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы

Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

8. Методические рекомендации для обучающихся по освоению дисциплины

Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала

(понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Б1.В.03 Защита информации от вредоносного программного обеспечения» для использования в 20___/20___ учебном году

Утверждаю

Зам. директора по УР _____
«___» _____ 20___ г.

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения: очная

(Возможны следующие варианты):

а) Рабочая программа действует без изменений.

б) В рабочую программу вносятся следующие изменения:

- 1)
- 2)
- 3)

Разработчик (и): _____
(ФИО, ученая степень, ученое звание)

«___» _____ 20___ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИВТ

Протокол № _____ от «___» _____ 20___ г.

Заведующий кафедрой _____

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	Уровень освоения компетенции	Критерии оценивания
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не	Обучающийся обнаруживает пробелы в знаниях основного учебного материала,

	достигнут	допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не знаком с рекомендованной литературой, не может исправить допущенные ошибки. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.
--	-----------	---

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания
ПК-3. Администрирование средств защиты информации прикладного и системного программного обеспечения		
Знать:		
методы ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования;	Контрольная работа	Модуль 1 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8 «Отлично» - 9-10
	Контрольная работа	Модуль 2 0÷14 «Неудовлетворительно» - 0-7 «Удовлетворительно» - 8-10 «Хорошо» - 11-12 «Отлично» - 13-14
Уметь:		
осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения;	Практические занятия 1-2	Модуль 10 0÷10 за каждое ПЗ «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8 «Отлично» - 9-10
	Лабораторные работы 1-6	Модуль 2 0÷3 за каждую ЛР «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
Владеть:		
навыками по обнаружению вредоносного программного обеспечения и ликвидации последствий его функционирования;	Практические занятия 3-4	Модуль 10 0÷10 за каждое ПЗ «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8 «Отлично» - 9-10
навыками установки, конфигурации и эксплуатации программного обеспечения по защите информации.	Лабораторные работы 7-12	Модуль 2 0÷3 за каждую ЛР «Неудовлетворительно» - 0 «Удовлетворительно» - 1

		«Хорошо» - 2 «Отлично» - 3
	Экзамен	0÷100 «Неудовлетворительно» - 0-40 «Удовлетворительно» - 41-60 «Хорошо» - 61-80 «Отлично» - 81-100

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные материалы текущего контроля для очной формы обучения

Данная дисциплина формирует у обучающегося 2 компетенции, которые связаны, взаимодействуют между собой и объективно оценить каждую в отдельности при ответе обучающегося на контрольный вопрос или при выполнении практического или лабораторного задания достаточно сложно. Предлагается считать, что вклад 2-х компетенций в общую оценку при ответе на вопрос примерно одинаков.

Модуль 1 (50 баллов):

Модуль содержит 4 лекционных и 4 практических занятия. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненные и защищенные практические занятия обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50 баллов.

Вопросы для контрольной работы (ПК-3):

1. Понятие вируса, классификация вирусов.
2. Вирусы загрузочные, файловые, полиморфные, стелс-вирусы, троянский конь.
3. Механизмы заражения компьютерными вирусами.
4. Признаки появления вирусов. Средства защиты от вирусов.
5. Антивирусные средства.
6. Алгоритм работы антивируса.
7. Понятие межсетевого экрана (МЭ), классы защищенности, основные компоненты.
8. Общие требования, предъявляемые к МЭ.
9. Основные функции МЭ.
10. Стратегия брандмауэра.
11. Аппаратные и программные брандмауэры.
12. Политика сетевого подключения и политика брандмауэра.
13. Спам. История, виды, способы распространения.
14. Борьба со спамом. Наиболее распространенные виды спама.
15. Фишинг данных, навязывание товаров/услуг.
16. Распространенные методики фишинга данных и возможные средства противодействия им.
17. Типы фишинговых атак.
18. Примеры мошенничества с электронной почтой.
19. Анатомия фишинговых писем.
20. Настройка фильтров спама и антифишинговые плагины в почте.

Практическая работа 1. Изучение структуры PE-файлов.

Контрольные вопросы (ПК-3):

1. Что такое PE-файл и почему его структура удобна для операционной системы?
2. Какие шаги выполняются загрузчиком операционной системы при загрузке PE-файла?
3. Какова роль таблицы импорта в процессе загрузки PE-файла?
4. Для чего предназначены атрибуты секций в PE-файле?
5. Почему имена секций различны у разных компиляторов?
6. Зачем нужен раздел с таблицей релокаций в PE-файле?
7. Какой основной базовый адрес указывается в большинстве исполняемых файлов?
8. В чём основная сложность при выборе базового адреса для динамических библиотек?
9. Что такое связывание (binding) функций в контексте загрузки программы?
10. Почему обычный механизм экспорта функций в сборках .NET применяется редко?

Практическая работа 2. Способы внедрения вредоносного кода.

Контрольные вопросы (ПК-3):

1. Какой основной способ заражения пользователей вредоносным ПО через социальную инженерию?
2. Чем привлекателен метод социальной инженерии для злоумышленников?
3. Приведите пример известного почтового червя, использовавшего технику социальной инженерии.
4. В чем заключалась стратегия привлечения внимания пользователей в случае червя LoveLetter?
5. Согласно какой организации почтовый червь LoveLetter занимает первое место по финансовому ущербу?
6. Что представляют собой уязвимости, которыми пользуются злоумышленники для внедрения вредоносного кода?
7. Почему современные операционные системы и приложения неизбежно содержат уязвимости?
8. Какие известные вирусы использовали уязвимости в почтовых клиентах Outlook?
9. Опишите механизм заражения компьютеров через заражённые веб-страницы.
10. Какие существуют виды троянских программ и какую роль они играют в распространении вредоносного ПО?

Практическая работа 3. Дизассемблирование.

Контрольные вопросы (ПК-3):

1. Дизассемблирование кода.
2. Какие традиционные инструменты используются при разработке программ?
3. Какие инструменты позволяют восстановить исходный текст программы?
4. Что представляют собой дизассемблеры и декомпиляторы?
5. Почему восстановление исходного текста программы является сложной задачей?
6. Объясните причины различия между исходным текстом оригинальной программы и результатом декомпиляции.
7. Цель инструментальных средств дизассемблирования.
8. Базовый алгоритм дизассемблирования.
9. Обязательно ли глубоко понимать механизмы дизассемблирования для эффективного использования дизассемблера?
10. Чего желательно избегать при работе над проектом обратного проектирования?

Практическая работа 4. Отладка кода.

Контрольные вопросы (ПК-3):

1. Что такое отладка программы и зачем она нужна?

2. Приведите пример ситуации, когда потребуется провести отладку.
3. Чем отладка отличается от тестирования программы?
4. Кто обычно проводит отладку программы?
5. Какие инструменты помогают выявлять ошибки в ходе отладки?
6. Кто обычно занимается отладкой программ помимо разработчиков?
7. Приведите пример простого случая, когда тестировщик сам исправляет ошибку в коде.
8. Какие распространенные ошибки встречаются в автоматических тестах?
9. Как сообщения об ошибках могут облегчить отладку программы?
10. Что значит «добавление отладочных сообщений»?

Модуль 2 (50 баллов):

Модуль содержит 2 лекционных занятия и 12 лабораторных работ. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 14. За выполненные и защищенные практические занятия обучающийся получает максимум 36 баллов. Общее максимальное количество баллов за модуль 2 составляет 50 баллов.

Вопросы для контрольной работы (ПК-3):

1. Модель системы защиты от вредоносных программ.
2. Технический компонент. Работа с файлом как с массивом байтов.
3. Модель системы защиты от вредоносных программ.
4. Технический компонент. Эмуляция кода программы.
5. Модель системы защиты от вредоносных программ.
6. Технический компонент. Запуск программы в «песочнице».
7. Модель системы защиты от вредоносных программ.
8. Технический компонент. Мониторинг системных событий.
9. Модель системы защиты от вредоносных программ.
10. Технический компонент. Поиск системных аномалий.
11. Модель системы защиты от вредоносных программ.
12. Аналитический компонент. Простое сравнение.
13. Модель системы защиты от вредоносных программ.
14. Аналитический компонент. Сложное сравнение.
15. Модель системы защиты от вредоносных программ.
16. Аналитический компонент. Экспертная система.
17. Методы и технологии защиты от вредоносного программного обеспечения.
18. Методы контроля доступа, основанные на разграничении доступа, различающиеся способами идентификации.
19. Модели, методы и средства контроля доступа к ресурсам вычислительных систем.
20. Методы контроля доступа с механизмами ограничения как: идентификация и аутентификация.

Лабораторная работа 1. Разработка компонента меж процессного взаимодействия.

Контрольные вопросы (ПК-3):

1. Что такое меж процессное взаимодействие (IPC)?
2. Перечислите основные способы меж процессного взаимодействия.
3. Как называются специализированные области памяти, доступные нескольким процессам одновременно?
4. Какой способ меж процессного взаимодействия позволяет процессам отправлять и получать сообщения последовательно?

5. Назовите тип сигналов, используемых для уведомления процессов о наступивших событиях.
6. Почему каждой операционной системе требуются специфические подходы к организации многозадачности?
7. Структура объекта исполняющей системы.
8. Что понимается под управлением объектов исполняющей системы?
9. Действия программиста для получения доступа к ресурсу.
10. Какие способы организации многозадачности ОС предоставляет программисту?

Лабораторная работа 2. Разработка компонента антивирусных баз.

Контрольные вопросы (ПК-3):

1. Особый подход к разработке антивирусов.
2. Движок антивирусного продукта, анализирующий поведение программ.
3. Базы данных с сигнатурами известных вредоносных объектов.
4. Из каких этапов состоит подготовка к выпуску новой версии антивирусного продукта?
5. Кто первым проводит тестирование новых правил антивирусных баз?
6. Проверка отсутствия ложных срабатываний на легитимное программное обеспечение.
7. Зачем необходима постоянная актуализация коллекции чистых файлов?
8. Что проверяется вторым типом тестов в процессе подготовки антивирусных баз?
9. Почему важно наличие разнообразия среди образцов вредоносного ПО в специальной библиотеке?
10. Методы обнаружения вредоносного кода.

Лабораторная работа 3. Разработка компонента сигнатурного сканирования.

Контрольные вопросы (ПК-3):

1. Поиск вредоносного объекта по сигнатурам.
2. Определения соответствия между некоторой сигнатурой и исследуемым файлом.
3. Каковы основные причины необходимости идентификации объектов в контексте информационной безопасности?
4. Какие конкретные задачи возникают при сравнении файлов или их частей в современной информационной сфере?
5. Почему традиционному сигнатурному анализу сложно справиться с современными модификациями вредоносного ПО?
6. Что означает понятие «семьи вредоносных программ»? И почему такая классификация полезна?
7. Какие дополнительные цели помимо выявления вредоносного ПО преследует процедура сравнения файлов?
8. Почему изменение сигнатуры файла может привести к непредсказуемым последствиям?
9. Объясните значение параметра "энтропия" файла и как он влияет на понимание содержимого файла.
10. Расчёт энтропии файла по формуле Клода Шеннона.

Лабораторная работа 4. Разработка компонента обнаружения и подготовки к сканированию исполняемых файлов.

Контрольные вопросы (ПК-3):

1. Существующие методы и подходы идентификации программного обеспечения.
2. Современные решения в области идентификации исполняемых файлов.
3. Подходы к идентификации исполняемых файлов.
4. Метод выделения признаков пространства исполняемых файлов с последующим созданием сигнатур на его основе.

5. Метод сравнения сигнатуры идентифицируемого исполняемого файла с эталонными сигнатурами программ.
6. Какие главные недостатки характерны для существующих методов идентификации программного обеспечения?
7. Почему существующие методы неэффективны при обработке незнакомых или редко встречающихся файлов?
8. Какую проблему представляет ограничение исследования преимущественно на PE-файловых форматах?
9. Какие возможности открывает разработка универсального метода идентификации, способного обрабатывать различные форматы исполняемых файлов?
10. Описание типов исполняемых файлов, их разрядности.

Лабораторная работа 5. Разработка компонента обнаружения и подготовки к сканированию архивов.

Контрольные вопросы (ПК-3):

1. Почему простого физического ограничения доступа к компьютеру недостаточно для полной защиты данных?
2. Что значит «физический доступ к компьютеру» и какими возможностями он наделяет злоумышленника?
3. Какие существуют альтернативные уровни защиты, если физические меры недостаточны?
4. Каким образом современные архиваторы помогают защитить конфиденциальную информацию?
5. Какие преимущества и ограничения имеются у метода шифрования посредством архиваторов?
6. Какие преимущества даёт прозрачное шифрование на уровне операционной системы?
7. Что произойдет, если вы забудете экспортировать ключ шифрования перед переустановкой системы?
8. Как осуществляется идентификация пользователя при шифровании с помощью EFS?
9. Какова роль «агента восстановления» в механизме EFS?
10. Как обезопасить себя от потери доступа к своим зашифрованным данным?

Лабораторная работа 6. Разработка компонента сканирования файлов и директорий по запросу.

Контрольные вопросы (ПК-3):

1. Как структурировать проект для поддержки подключаемых модулей?
2. Как правильно загружать и создавать экземпляры команд из загруженных сборок подключаемого модуля?
3. Вероятные конфликты при подключении модулей.
4. Как настроить параметры сканирования антивирусом?
5. Как настроить сканирование с использованием командной строки?
6. Пользовательское сканирование с указанием директорий, которые необходимо сканировать.
7. Как настроить исключения для сканирования?
8. Автоматическое помещение файлов при сканировании системы в карантин.
9. Как восстановить элементы, заблокированные антивирусом?
10. Что такое разрешенные угрозы?

Лабораторная работа 7. Разработка компонента сканирования файлов и директорий по расписанию.

Контрольные вопросы (ПК-3):

1. Как создать простой подключаемый модуль без зависимостей?

2. Как создать подключаемый модуль с зависимостями библиотеки?
3. Какие возможности предоставляют фреймворки подключаемых модулей для расширения функционала приложений и библиотек?
4. Как запланировать полное сканирование?
5. Как запланировать периодическое полное сканирование?
6. Как работает Библиотека планировщика заданий?
7. Как задать сканирование при запуске системы?
8. На что влияет повторяемость проверок?
9. Как включить или выключить оповещения системы сканирования?
10. Настройки сканирования при неактивном компьютере.

Лабораторная работа 8. Разработка компонента мониторинга директорий.

Контрольные вопросы (ПК-3):

1. Почему мониторинг директорий важен для автоматизации процессов управления файлами?
2. Какие ключевые критерии необходимо учесть при постановке задачи по разработке компонента мониторинга директорий?
3. Перечислите доступные технологии мониторинга файлов и папок для операционных систем Linux и Windows.
4. Объясните разницу между inotify и ReadDirectoryChangesW API в плане мониторинга изменений в файловой системе.
5. Зачем нужен отдельный поток или процесс для мониторинга файлов в приложении?
6. Каковы преимущества использования очереди сообщений для обработки событий в компоненте мониторинга директорий?
7. Приведите пример сценария тестирования функциональности компонента мониторинга директорий.
8. Какие факторы влияют на производительность компонента мониторинга директорий и как их оптимизировать?
9. Опишите возможные способы интеграции компонента мониторинга директорий с существующими системами.
10. Какие дополнительные меры защиты рекомендуется применять при разработке компонентов мониторинга файлов и папок?

Лабораторная работа 9. Разработка компонента «Карантин».

Контрольные вопросы (ПК-3):

1. Что такое компонент «Карантин» и зачем он необходим в современных антивирусных программах?
2. Какие функциональные и нефункциональные требования учитываются при создании компонента «Карантин»?
3. Почему важно поддерживать разнообразные типы файлов в компоненте «Карантин»?
4. Опишите архитектуру компонента «Карантин»: какие модули входят в его структуру, и какова их функциональность?
5. Какой модуль отвечает за хранение и защиту изолированных файлов в компоненте «Карантин»?
6. Расскажите о механизме обнаружения вредоносных элементов в компоненте «Карантин».
7. Зачем необходима система уведомлений в компоненте «Карантин», и какие события она должна фиксировать?
8. Какие тесты используются для оценки качества и работоспособности компонента «Карантин»?
9. Какие меры предосторожности принимаются для защиты и конфиденциальности хранящихся в карантине файлов?

10. Какое значение имеет регулярное резервное копирование базы данных в компоненте «Карантин»?

Лабораторная работа 10. Разработка компонента персистентного хранения настроек.

Контрольные вопросы (ПК-3):

1. Что такое компонент персистентного хранения настроек и зачем он нужен в современных приложениях?
2. Какие существуют базовые требования к такому компоненту и как они формулируются на этапе постановки задачи?
3. Какие факторы определяют выбор конкретной архитектуры для компонента персистентного хранения настроек?
4. Назовите несколько распространённых инструментов и технологий, используемых для реализации персистентного хранения настроек.
5. Из каких основных функциональных блоков состоит компонент персистентного хранения настроек и какие задачи решает каждый из них?
6. Какие дополнительные функции необходимы помимо базовых операций чтения и записи данных?
7. Какие тестовые сценарии важны для полноценного тестирования компонента персистентного хранения настроек?
8. Приведите примеры ситуаций, которые требуют дополнительного внимания при межплатформенных испытаниях компонента?
9. Какие важные моменты необходимо отразить в документации компонента персистентного хранения настроек?
10. Как грамотно интегрировать созданный компонент в существующее приложение, и какие подводные камни могут встретиться в процессе интеграции?

Лабораторная работа 11. Разработка компонента персистентного хранения отчетов о сканировании.

Контрольные вопросы (ПК-3):

1. Что такое компонент персистентного хранения отчетов о сканировании и для чего он нужен?
2. Какие основные задачи ставятся перед компонентом на начальном этапе разработки?
3. Какие существуют подходы к выбору технологии хранения отчетов о сканировании?
4. В чём разница между реляционными и NoSQL-базами данных применительно к задаче хранения отчетов о сканировании?
5. Какие преимущества даёт файловое хранилище (JSON/XML) в сравнении с реляционной базой данных?
6. Какие аспекты нужно учитывать при проектировании схемы данных для отчета о сканировании?
7. Какие ключевые функции должны присутствовать в компоненте персистентного хранения отчетов о сканировании?
8. Как организовать эффективную фильтрацию и сортировку отчетных данных?
9. Какие меры безопасности необходимы для надежного хранения отчетов о сканировании?
10. Как осуществляется интеграция компонента персистентного хранения отчетов с системой сканирования?

Лабораторная работа 12. Создание графического пользовательского интерфейса.
Контрольные вопросы (ПК-3):

1. Что такое графический пользовательский интерфейс (GUI)?

2. Какие задачи решаются на этапе анализа потребностей и целевых пользователей при разработке GUI?
3. Какие элементы составляют концепцию графического интерфейса на этапе концептуального проектирования?
4. Какие современные инструменты и фреймворки применяются для программирования графического интерфейса?
5. Почему важно проводить тестирование графического интерфейса на реальных пользователях?
6. Какие мероприятия выполняются на завершающем этапе подготовки интерфейса к релизу?
7. В чём заключается важность этапа анализа потребностей и исследования конкурентов при создании GUI?
8. Какие бывают типы элементов управления в графическом интерфейсе?
9. Чем отличаются этапы концептуального проектирования и дизайна графического интерфейса?
10. Как технология A/B-тестирования помогает выбрать лучший вариант исполнения элементов интерфейса?

1.3.2 Вопросы, выносимые на экзамен по дисциплине «Защита информации от вредоносного программного обеспечения» (ПК-3) (промежуточная аттестация)

1. Понятие вируса, классификация вирусов.
2. Вирусы загрузочные, файловые, полиморфные, стелс-вирусы, троянский конь.
3. Механизмы заражения компьютерными вирусами.
4. Признаки появления вирусов. Средства защиты от вирусов.
5. Антивирусные средства.
6. Алгоритм работы антивируса.
7. Понятие межсетевого экрана (МЭ), классы защищенности, основные компоненты.
8. Общие требования, предъявляемые к МЭ.
9. Основные функции МЭ.
10. Стратегия брандмауэра.
11. Аппаратные и программные брандмауэры.
12. Политика сетевого подключения и политика брандмауэра.
13. Спам. История, виды, способы распространения.
14. Борьба со спамом. Наиболее распространенные виды спама.
15. Фишинг данных, навязывание товаров/услуг.
16. Распространенные методики фишинга данных и возможные средства противодействия им.
17. Типы фишинговых атак.
18. Примеры мошенничества с электронной почтой.
19. Анатомия фишинговых писем.
20. Настройка фильтров спама и антифишинговые плагины в почте.
21. Модель системы защиты от вредоносных программ.
22. Технический компонент. Работа с файлом как с массивом байтов.
23. Модель системы защиты от вредоносных программ.
24. Технический компонент. Эмуляция кода программы.
25. Модель системы защиты от вредоносных программ.
26. Технический компонент. Запуск программы в «песочнице».
27. Модель системы защиты от вредоносных программ.
28. Технический компонент. Мониторинг системных событий.

29. Модель системы защиты от вредоносных программ.
30. Технический компонент. Поиск системных аномалий.
31. Модель системы защиты от вредоносных программ.
32. Аналитический компонент. Простое сравнение.
33. Модель системы защиты от вредоносных программ.
34. Аналитический компонент. Сложное сравнение.
35. Модель системы защиты от вредоносных программ.
36. Аналитический компонент. Экспертная система.
37. Методы и технологии защиты от вредоносного программного обеспечения.
38. Методы контроля доступа, основанные на разграничении доступа, различающиеся способами идентификации.
39. Модели, методы и средства контроля доступа к ресурсам вычислительных систем.
40. Методы контроля доступа с механизмами ограничения как: идентификация и аутентификация.

2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Порядок и методика проведения текущего контроля и промежуточной аттестации

Предусмотрены следующие виды контроля:

- текущий контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;
- текущий контроль по каждому модулю – в форме отчетов по лабораторным работам и практическим занятиям для оценки практических навыков;
- промежуточная аттестация по дисциплине – в форме экзамена.

Текущий контроль успеваемости в форме защиты лабораторных и практических проводится в два этапа:

- 1-й этап: допуск к выполнению лабораторной работы – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний обучающихся теоретической части лабораторной работы и готовности к выполнению практических исследований;
- 2-й этап выполняется по окончании каждой лабораторной работы (практического занятия) в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки обучающимся практических навыков исследования на аппаратуре.

Контрольные работы выполняются в виде короткого письменного ответа на один вопрос, изученный на предыдущей лекции в начале каждой последующей лекции. Ответ на вопрос дается в течение 5-10 минут. Таким образом, после лекционного курса каждого модуля формируется общая оценка за теоретические знания.

С целью повышения качества обучения за счет побуждения обучающихся к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности обучающихся в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимися в рамках текущего контроля баллы могут быть переведены в оценку:

- «неудовлетворительно» - от 0 до 40 от максимального количества баллов;

- «удовлетворительно» - от 41 до 60 максимального количества баллов;
- «хорошо» - от 61 до 80 максимального количества баллов;
- «отлично» - от 81 до 100 максимального количества баллов.

Соотношения максимального количества баллов, полученных обучающимся по блокам модулей, показаны в Таблице 1.

Таблица 1 - Распределение баллов по модулям дисциплины «Защита информации от вредоносного программного обеспечения»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок
Модуль 1	50	10	40
Модуль 2	50	14	36
Экзамен	100		

Как правило, теоретический блок оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения лабораторных работ и заданий на практических занятиях.

На экзамене производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуется формировать вопросы в экзаменационных билетах таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

3. Промежуточная аттестация

Промежуточная аттестация проводится в форме экзамена. Экзамен проводится по расписанию промежуточной аттестации в устном виде по экзаменационным билетам. Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

Образец экзаменационного билета

	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 И.о.зав. кафедрой «ИБ» _____ А.Г.Жуковский «___» _____ 20__ г.
	Направление подготовки: 10.03.01 Информационная безопасность Курсы: 3 Дисциплина: Защита информации от вредоносного программного обеспечения	
Билет №1 1. Механизмы заражения компьютерными вирусами. 2. Модель системы защиты от вредоносных программ. К.т.н., доцент _____ Маршаков Д.В. «___» _____ 20__ г.		

Один комплект отпечатанных экзаменационных билетов, подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

4 Тестовые задания по дисциплине «Защита информации от вредоносного программного обеспечения»

Тестовые задания позволяют оценить уровень сформированности компетенции ПК-3.

Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень содержит примерно 50 % заданий.

Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.).

Повышенный уровень в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности.

Высокий уровень в среднем составляют – 15 % заданий.

В заданиях используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий по компетенции равно 20.

Один комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

ПК-3. Администрирование средств защиты информации прикладного и системного программного обеспечения

БЛОК А (базовый уровень) – задание с выбором одного или нескольких верных ответов из предложенных вариантов.

Инструкция по тестам Блока А: прочитайте текст и выберите один или несколько правильных ответов.

№ задания	Тексты заданий
1	Что такое антивирусное программное обеспечение? 1. Программное обеспечение для защиты систем от вирусов. 2. Программное обеспечение для шифрования данных. 3. Программное обеспечение для контроля доступа. 4. Программное обеспечение для аутентификации пользователей.
2	Какие меры безопасности могут быть связаны с физическими преградами? 1. Установка видеонаблюдения и систем контроля доступа 2. Использование мощных шифровальных алгоритмов для защиты данных 3. Усиление физической защиты зданий и помещений 4. Все перечисленное выше
3	Что такое техническая защита информации? 1. Защита информации с использованием криптографических методов 2. Защита информации с использованием технических, программных и программно-технических средств 3. Защита информации с использованием физических преград 4. Защита информации с использованием социальных мер безопасности
4	Какие задачи решает техническая защита информации? 1. Предотвращение утечки информации через технические каналы утечки информации 2. Предотвращение несанкционированного доступа к информации 3. Обеспечение целостности, конфиденциальности и доступности защищаемой информации 4. Все перечисленное выше
5	Какие основные категории угроз информационной безопасности существуют? 1. Технические угрозы 2. Организационные угрозы 3. Персональные угрозы 4. Все перечисленное выше
6	Какие преимущества обеспечения безопасности сетевых соединений с помощью виртуальных частных сетей (VPN)?

№ задания	Тексты заданий
	1. Шифрование данных для защиты конфиденциальности 2. Обеспечение анонимности пользователя 3. Позволяет подключаться к защищенным сетям удаленно 4. Предотвращение перехвата данных в общественных Wi-Fi сетях
7	Что такое защита от атак по сети и почему она важна? 1. Обеспечение безопасности сетевых соединений и защита от несанкционированного доступа 2. Защита от физических угроз и контроль доступа в помещения 3. Шифрование данных и защита от вредоносного программного обеспечения 4. Отслеживание активности пользователей и аудит безопасности
8	Какие методы аутентификации могут использоваться для проверки подлинности пользователя? 1. Логин и пароль, биометрические данные, одноразовые коды 2. Антивирусное программное обеспечение, фаерволы, VPN 3. Криптографические алгоритмы, сетевые протоколы, защитные меры 4. Контроль доступа, системы мониторинга, физические барьеры
9	Что такое авторизация и почему она важна в контексте информационной безопасности? 1. Проверка прав доступа пользователя к определенным ресурсам 2. Шифрование данных для защиты от несанкционированного доступа 3. Контроль целостности информации и предотвращение ее изменения 4. Анализ угроз и реагирование на них в реальном времени
10	Что такое уровень целостности данных? 1. Способность данных быть доступными только для авторизованных пользователей 2. Способность данных оставаться неизменными и быть защищенными от несанкционированного изменения 3. Способность данных быть достоверными и точными 4. Способность данных быть сохраненными и доступными в случае сбоя системы

БЛОК Б (повышенный уровень) – задание закрытого типа на установление соответствия

Инструкция: Прочитайте текст и установите соответствие.

№ задания	Тексты заданий
11	Установите соответствие между типами данных и примерами данных: 1. Персональные данные 2. Конфиденциальные данные 3. Открытые данные 4. Коммерческая тайна А) Публичные статистические данные Б) Паспортные данные В) Финансовые отчеты компании Г) Медицинская история пациента
12	Установите соответствие между технологиями и их функциями в цифровом праве: 1. Шифрование 2. Файрвол 3. Антивирус 4. Двухфакторная аутентификация А) Защита от вредоносного ПО Б) Дополнительный уровень проверки личности В) Защита данных путем кодирования Г) Защита сетевого периметра
13	Установите соответствие между правами в области цифрового права и их примерами: 1. Право на доступ к информации 2. Право на забвение 3. Право на защиту данных 4. Право на исправление данных А) Исправление неточной или неполной информации Б) Защита данных от несанкционированного доступа В) Удаление персональных данных по запросу пользователя

№ задания	Тексты заданий
	Г) Получение копии данных, хранящихся о пользователе
14	Установите соответствие между нормативными документами и их назначением: 1. GDPR (General Data Protection Regulation) 2. Закон "О персональных данных" 3. Закон "Об электронной подписи" 4. Закон "О коммерческой тайне" А) Защита конфиденциальной информации компании Б) Регулирование обработки персональных данных в Европе В) Регулирование обработки персональных данных в России Г) Регулирование использования электронной подписи

БЛОК Б (повышенный уровень) – задание закрытого типа на установление последовательности.

Инструкция: Прочитайте текст и установите правильную последовательность.

№ задания	Тексты заданий
15	Расположите примеры персональных данных согласно уровня защищённости от минимального риска к высокому: 1. контактные телефоны сотрудников компаний 2. электронная почта, указанная на сайте компании 3. биометрические данные клиента 4. паспорт гражданина РФ
16	Расположите объекты атак методом социальной инженерии по их популярности: 1. социальные сети 2. электронная почта 3. мессенджеры 4. сайты
17	Расположите этапы стадии создания системы защиты информации в правильном порядке: 1. Разработка системы защиты информации. 2. Подтверждение соответствия системы защиты информации. 3. Внедрение системы защиты информации. 4. Формирование требований к системе защиты информации.

БЛОК В (высокий уровень) – задание открытого типа с развернутым ответом.

Инструкция: Прочитайте текст и запишите обоснованный ответ.

№ задания	Тексты заданий
18	Процедура подтверждения прав пользователей на доступ к определенным ресурсам или функциям системы. Она представляет собой этап проверки учетных данных и допуска к выполнению определенных действий. Эта процедура называется _____
19	Федеральный орган исполнительной власти, который разрабатывает и утверждает российские стандарты (ГОСТы) называется Федеральное агентство по техническому регулированию и метрологии или _____.
20	Согласно приказа Роскомнадзора № 179 об утверждении «Требований к подтверждению уничтожения персональных данных», если обработка персональных данных осуществляется оператором без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов, является _____.

Система оценивания выполнения тестовых заданий по компетенции ПК-3

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует - 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

Перед началом изучения дисциплины преподаватель должен ознакомить обучающихся с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

- 1) формулирует тему и цель занятия, объявляет учебные вопросы;
- 2) излагает основные теоретические положения;
- 3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;
- 4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;
- 5) в конце занятия выдает вопросы для самостоятельного изучения.

На занятиях лабораторного цикла следует обратить внимание на соответствие выбираемых обучающимся средств выполнения решаемым в работе задачам.

Каждая лабораторная работа должна быть оформлена и защищена в соответствии с требованиями. Защита производится после оформления отчета по работе.

Во время выполнения заданий в учебной аудитории обучающийся может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, обучающийся может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего контроля и промежуточной аттестации знаний обучающихся.

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, обучающиеся должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы обучающегося на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности обучающихся.

2.2 Методические указания для обучающихся по подготовке к лабораторным работам

Лабораторные занятия по любой учебной дисциплине проводятся в соответствии с рабочей программой этой учебной дисциплины в установленные расписанием часы.

Инструктаж по технике безопасности, правилам пожарной безопасности и правилам внутреннего распорядка в лаборатории проводится преподавателем на первом лабораторном занятии. На этом же занятии обучающимся сообщаются:

- программа всего предстоящего лабораторного цикла;
- условия взаимодействия обучающихся с преподавателем в процессе выполнения лабораторных работ;
- условия контроля самостоятельной работы обучающихся, включая правила оформления отчетов по лабораторным работам и их последующей защиты;
- другая необходимая информация.

Организация лабораторных работ включает:

- самостоятельную внеаудиторную подготовку обучающегося к выполнению каждой отдельной лабораторной работы в соответствии с ее программой в рамках часов, выделенных на самостоятельную проработку материала в программе дисциплины;
- входной контроль преподавателем степени подготовленности каждого обучающегося к выполнению лабораторных работ;
- выполнение программы лабораторных работ в полном объеме;
- оформление отчета и его защиту каждым обучающимся в установленные сроки;
- формирование преподавателем рейтингов каждого из обучающихся по результатам выполнения и защиты им отдельных лабораторных работ и их циклов (используется Модульно-рейтинговая система).

Оценка качества выполнения лабораторных работ каждым обучающимся производится преподавателем отдельно за подготовку к работе, ее выполнение и защиту.

2.3 Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

- изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д.;
- при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа обучающегося под управлением преподавателя. На них пополняются теоретические знания обучающихся, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение обучающихся к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы.

После подведения итогов занятия обучающийся обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

Методические указания по выполнению лабораторных и практических работ по дисциплине «*Защита информации от вредоносного программного обеспечения*» для обучающихся очной формы обучения, размещенные на сайте СКФ МТУСИ в разделе «Методические материалы».

3. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа обучающихся 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.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к лабораторным работам (практическим занятиям);
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях.
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов по отдельным вопросам изучаемой дисциплины.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Обычно постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятии, предшествующему данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.

Самостоятельная работа обучающихся над усвоением материала по дисциплине может выполняться в помещении для самостоятельной работы СКФ МТУСИ, посредством использования электронной библиотеки и ЭИОС.