

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» 04 2026 г.

Рабочая программа дисциплины

**Б1.В.04 Разработка безопасного программного обеспечения
(Проектирование защищенных информационных систем)**

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):	3	108/5
Контактная работа, в том числе (по семестрам, курсам):		50/5
Лекции		18/5
Лабораторных работ		16/5
Практических занятий		16/5
Семинаров		
Самостоятельная работа		22/5
Контроль		36/5
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		1/5

Программу составил:

Кандидат технических наук Швидченко С.А.

Рабочая программа дисциплины

«Разработка безопасного программного обеспечения (Проектирование защищенных информационных систем)»

Разработана в соответствии с ФГОС ВО

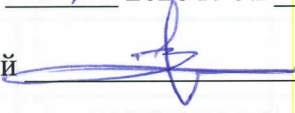
направлением подготовки **10.03.01 Информационная безопасность**, утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427.

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

Целью освоения дисциплины «Разработка безопасного программного обеспечения» является получение обучающимися знаний, формирование у них умений и навыков, необходимых при разработке безопасного программного обеспечения для решения задач в профессиональной деятельности, соответствующих общепрофессиональных компетенций в соответствии с ООП, а также основных знаний и умений в области разработки безопасного 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 следующие компетенции:

ПК-1. Администрирование подсистем защиты информации в операционных системах
Знать:
Архитектуру и принципы построения операционных систем. Программные интерфейсы операционных систем. Архитектуру подсистем защиты информации в операционных системах. Принципы функционирования средств защиты информации в операционных системах. Нормативные правовые акты в области защиты информации. Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. Правила эксплуатации программно-аппаратных средств защиты информации; Организационные меры по защите информации.
Уметь:
Формулировать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах.
Владеть:
Навыками определения состава применяемых программно-аппаратных средств защиты информации в операционных системах. Навыками разработки порядка применения программно-аппаратных средств защиты информации в операционных системах. Навыками формирования шаблонов установки программно-аппаратных средств защиты информации в операционных системах.
ПК-2. Администрирование программно-аппаратных средств защиты информации в компьютерных сетях
Знать:
- информационно-коммуникативные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, и принципы их применения при решении задач профессиональной деятельности; - особенности безопасной разработки на фазе тестирования ПО; - особенности безопасной разработки на фазах выпуска и поддержки ПО; - инструментальные средства разработки безопасных программ.
Уметь:
Подбирать информационно-коммуникативные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности Обеспечивать безопасную разработку на фазе тестирования ПО;

Обеспечивать безопасную разработку на фазах выпуска и поддержки ПО; Использовать инструментальные средства разработки безопасных программ
Владеть:
- навыками применения информационно-коммуникативных технологий, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности; - навыками нахождения уязвимостей ОС; - навыками защиты ПО от копирования переносными носителями; - навыками обнаружения вредоносного программного обеспечения и безопасной работы в интернет.

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.31	Защита информации от утечки по техническим каналам
3	Б1.В.02	Комплексное обеспечение защиты информации объекта информатизации
4	Б1.О.36.03	Безопасность компьютерных сетей
5	Б1.О.36.06	Администрирование средств защиты информации в компьютерных системах и сетях
6	Б1.О.33	Программно-аппаратные средства защиты информации

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. час.	Компетенции	УМИО
1	2	3	4	5	6
Курс 3, Семестр 5 – 50 часов аудиторных занятий + 22 часа СРС + контроль 36 ч. = 108 часов					
Модуль 1. Основные понятия угроз и уязвимостей информационной безопасности при разработке ПО (26 + 12 = 38 часов)					
1.1	Лекция 1. Введение в дисциплину. Базовая терминология. Угрозы и уязвимости информационной безопасности при разработке ПО. Безопасное ПО. Тестирование и анализ ПО. Фаззинг. Инструментальные среды и средства разработки и анализа ПО. Управление конфигурацией ПО. Документация разработчика ПО. Цели создание безопасного ПО и меры по их достижению.	Лек.	2	ПК-1; ПК-2	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3 Л2.4
1.2	Алгоритмы шифрования данных.	ПЗ	4	ПК-1; ПК-2	Л1.1, Л3.2
1.3	Методы поиска и сбора информации. Методика устранения компьютерной информации.	ЛР	2	ПК-1; ПК-2	Л1.1, Л1.2, Л3.1

1.4	1. Знакомство с ГОСТ Р 56939-2016 2. Формирование требований к ПО и составление технического задания с учетом требований ГОСТ Р 56939-2016 3. Принципы безопасной разработки. Построение модели угроз.	СРС	4	ПК-1; ПК-2	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3 Л2.4
1.5	Лекция 2. Основные нормативно-правовые акты в области создания безопасного ПО Обзор основных ГОСТов: - ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения; - ГОСТ Р 56546-2015 Классификация уязвимостей информационных систем; - ГОСТ Р 58412-2019 Защита информации. Разработка безопасного ПО. Угрозы безопасности информации при разработке ПО; - ГОСТ Р ИСО/МЭК 18045-2013 Методология оценки безопасности информационных технологий; - ГОСТ Р ИСО-МЭК 27034-1 Информационные технологии. Безопасность приложений. Часть 1. Безопасность приложений; - ГОСТ Р ИСО-МЭК 27034-7-2020 Информационные технологии. Безопасность приложений. Часть 7. Основы прогнозирования доверия	Лек.	4	ПК-1; ПК-2	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3 Л2.4
1.6	Защита от копирования	ПЗ	2	ПК-1; ПК-2	Л1.1, Л3.2,
1.7	Уязвимости WINDOWS. Защита от копирования переносных Носителей.	ЛР	4	ПК-1; ПК-2	Л1.1, Л1.2, Л2.1 Л3.1
1.8	1. Реализация ПО. Анализ кода уязвимого приложения 2. Тестирование ПО на изменение плоскости атак. 3. Планирование реагирования на инциденты. 4. Фазинг-тестирование ПО.	СРС	4	ПК-1; ПК-2	Л1.1, Л1.2, Л2.1
1.9	Лекция 3. Угрозы, уязвимости, риски информационной безопасности при разработке ПО - их выявление и оценка. Угрозы безопасности информации при разработке ПО (по ГОСТ Р 58412-2019). Классификация уязвимостей информационных систем (по ГОСТ Р 56546—2015). Выявление угроз безопасности информации при разработке ПО. Оценка уровня доверия безопасности ПО (степени соответствия выявленной безопасности ПО предъявленным требованиям) (по ГОСТ Р ИСО-МЭК 27034-7). Методы и средства оценки рисков информационной безопасности при создании ПО.	Лек.	4	ПК-1; ПК-2	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3 Л2.4
1.10	Защита от побочного электромагнитного излучения и	ПЗ	2	ПК-1; ПК-2	Л1.1, Л1.2, Л2.1

	наводок.				ЛЗ.1
1.11	Модели распространения программного Обеспечения	ЛР	2	ПК-1; ПК-2	Л1.1, Л1.2, Л2.1 ЛЗ.1
1.12	1. Принципы безопасной разработки. Построение модели угроз 2. Тестирование ПО на изменение плоскости атак 3. Планирование реагирования на инциденты.	СРС	4	ПК-1; ПК-2	Л1.1, Л1.2, Л2.1 Л2.2
Модуль 2. Безопасная разработка программного обеспечения (ПО) – (24 + 10 = 34 часа)					
2.1	Лекция 4. Организационные и технические меры по разработке безопасного ПО, реализуемых на различных стадиях жизненного цикла разработки безопасного ПО Меры по разработке безопасного ПО, реализуемые при выполнении анализа требований к ПО. Меры по разработке безопасного ПО, реализуемые при выполнении проектирования архитектуры ПО. Меры по разработке безопасного ПО, реализуемые при выполнении конструирования и комплексирования ПО. Меры по разработке безопасного ПО, реализуемые при выполнении квалификационного тестирования ПО. Меры по разработке безопасного ПО, реализуемые при выполнении инсталляции ПО и поддержки приемки ПО. Меры по разработке безопасного ПО, реализуемые при решении проблем в программном обеспечении в процессе эксплуатации. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента документацией и конфигурацией программы. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента инфраструктурой среды разработки ПО. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента людскими ресурсами. Меры по разработке безопасного ПО, реализуемые при выполнении.	Лек.	4	ПК-1; ПК-2	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3 Л2.4
2.2	Виды шифров. Алгоритмы распределения ключей	ПЗ	2	ПК-1; ПК-2	Л1.1, ЛЗ.2,
2.3	Аппаратные ключи защиты. Количественная оценка стойкости Парольной защиты.	ЛР	2	ПК-1; ПК-2	Л1.1, Л2.1 ЛЗ.1
2.4	Лекция 5. Тестирование и анализ ПО Виды тестирования ПО. Статический анализ ПО. Динамический анализ ПО. Защита ПО от взлома и несанкционированного использования	Лек.	2	ПК-1; ПК-2	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3
2.5	Симметричные алгоритмы	ПЗ	2	ПК-1; ПК-2	Л1.1, ЛЗ.1
2.6	Вредоносное программное обеспечение. Безопасная работа в интернет	ЛР	2	ПК-1; ПК-2	Л1.1, ЛЗ.1
2.7	1. Отечественные и зарубежные стандарты в области	СРС	5	ПК-1;	Л1.1,

	разработки безопасного ПО. 2. Обеспечение безопасной разработки на фазе формирования требований к ПО. 3. Обеспечение безопасной разработки на фазе проектирования ПО.			ПК-2	Л1.2, Л2.1 Л2.2 Л2.3
2.8	Лекция 6. Инструментальные средства разработки безопасных программ Инструментальные средства для безопасной разработки в среде Windows: - Microsoft Threat Modeling Tool 2014 — средство моделирования атак; - SDL MiniFuzz File Fuzzer — средство фаззинг-тестирования; - Attack Surface Analyzer — анализатор плоскости атаки; - Анализатор кода C/C++ из состава Microsoft VisualStudio.	Лек.	2	ПК-1; ПК-2	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3
2.9	Асимметричные алгоритмы	ПЗ	4	ПК-1; ПК-2	Л1.1, Л3.1
2.10	Обеспечение безопасности локальной сети. Настройка параметров. Безопасности браузера .	ЛР	4	ПК-1; ПК-2	Л1.1, Л3.1
2.11	1. Обеспечение безопасной разработки на фазе реализации ПО 2. Обеспечение безопасной разработки на фазе тестирования ПО 3. Обеспечение безопасной разработки на фазах выпуска и поддержки ПО	СРС	5	ПК-1; ПК-2	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3
	Экзамен		36	ПК-1; ПК-2	Л1.1, Л1.2, Л2.1 Л2.2 Л2.3 Л2.4 Л3.1
	Итого		108		

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	Грекул, В. И., Г. Н. Денищенко, Н. Л. Коровкина	Проектирование информационных систем: учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 299 с.	Э1
Л1.2	Онокой, Л. С., О. А. Морозова, Т. Е. Точилкина	Проектирование информационных систем : учебное пособие	Москва: Прометей, 2024. — 352 с.	Э2
5.1.2 Дополнительная литература				
Код	Авторы,	Заглавие	Издательство,	Кол.

	составители		год	
Л2.1	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2024. — 214 с.	Э3
Л2.2	В. В. Воронина, А. В. Михеев, Н. Г. Ярушкина, К. В. Святков	Теория и практика машинного обучения: учебное пособие	Ульяновск: Ульяновский государственный технический университет, 2017. — 291 с.	Э4
Л2.3	Гулько, А. В.	Системное программирование в среде Linux: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2020. — 235 с.	Э5
Л2.4	В.Г. Карташевский, Б. Я. Лихтциндер, Н. В. Киреева, М. А. Буранова	Компьютерные сети: учебник	Самара: Поволжский государственный университет телекоммуникаций и информатики, 2016. — 267 с.	Э6

5.1.3 Методическое обеспечение

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Зубкова, Т. М.	Технология разработки программного обеспечения: учебное пособие	Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2017. — 469 с.	Э7

5.2 Электронные образовательные ресурсы

Э1	https://www.iprbookshop.ru/142298.html
Э2	https://www.iprbookshop.ru/153542.html
Э3	https://www.iprbookshop.ru/142805.html
Э4	https://www.iprbookshop.ru/106120.html
Э5	https://www.iprbookshop.ru/98735.html
Э6	https://www.iprbookshop.ru/71846.html
Э7	https://www.iprbookshop.ru/78846.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)
5.3.6	Национальный открытый университет «ИНТУИТ» - https://intuit.ru/
5.3.7	Электронный ресурс http://www.securitylab.ru/

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

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная интерактивной доской, проектором, ПК (ноутбуком), экраном.
6.2 МТО лабораторных работ и практических занятий	
1	Лаборатория «Вычислительной техники и информатики», укомплектованная специализированной мебелью, оборудованная компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
2	Лаборатория «Программно-аппаратные средства защиты информации», укомплектованная специализированной мебелью, оснащенную программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации,
3	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, прочесть задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Б1.В.04 Разработка безопасного программного обеспечения (Проектирование защищенных информационных систем)» 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 ИБ

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 достигнут	Обучающийся обнаруживает пробелы в знаниях основного учебного материала, 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-1: Администрирование подсистем защиты информации в операционных системах		
Знать:		
– принципы функционирования средств защиты информации в операционных системах; – нормативные правовые акты в области защиты информации; – руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; – правила эксплуатации программно-аппаратных средств защиты информации;	Контрольная работа	Модуль 1 0÷7 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4 «Хорошо» - 5-6 «Отлично» - 7
– архитектуру и принципы построения операционных систем; – программные интерфейсы операционных систем; – архитектуру подсистем защиты информации в операционных системах; – организационные меры по защите информации.	Контрольная работа	Модуль 2 0÷7 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4 «Хорошо» - 5-6 «Отлично» - 7
Уметь:		
– формулировать политики безопасности операционных систем; – оценивать угрозы безопасности информации операционных систем;	Практические занятия 1-2	Модуль 1 0÷6 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4-5 «Отлично» - 6
– устанавливать обновления программного обеспечения и средств антивирусной защиты; – проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах.	Практические занятия 4	Модуль 2 0÷6 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4-5 «Отлично» - 6
Владеть:		
– навыками определения состава применяемых программно-аппаратных средств защиты информации в операционных системах; – навыками разработки порядка применения программно-аппаратных средств защиты информации в операционных системах;	Практические занятия 3	Модуль 1 0÷6 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4-5 «Отлично» - 6
– навыками формирования шаблонов установки программно-аппаратных средств защиты информации в операционных системах.	Практические занятия 5-6	Модуль 2 0÷6 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4-5

		«Отлично» - 6
ПК-2: Администрирование программно-аппаратных средств защиты информации в компьютерных сетях		
Знать:		
– информационно-коммуникативные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, и принципы их применения при решении задач профессиональной деятельности;	Контрольная работа	Модуль 1 0÷7 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4 «Хорошо» - 5-6 «Отлично» - 7
- особенности безопасной разработки на фазе тестирования ПО; - особенности безопасной разработки на фазах выпуска и поддержки ПО; – - инструментальные средства разработки безопасных программ.	Контрольная работа	Модуль 2 0÷7 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4 «Хорошо» - 5-6 «Отлично» - 7
Уметь:		
– подбирать информационно-коммуникативные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	Лабораторные работы 1-2	Модуль 1 0÷6 за каждую ЛР «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4-5 «Отлично» - 6
– обеспечивать безопасную разработку на фазе тестирования ПО; – обеспечивать безопасную разработку на фазах выпуска и поддержки ПО; – использовать инструментальные средства разработки безопасных программ.	Лабораторные работы 4	Модуль 2 0÷6 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4-5 «Отлично» - 6
Владеть:		
– навыками применения коммуникативных технологий, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	Лабораторные работы 3	Модуль 1 0÷6 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4-5 «Отлично» - 6
– навыками нахождения уязвимостей OS; – навыками защиты ПО от копирования переносными носителями; – навыками обнаружения вредоносного программного обеспечения и безопасной работы в интернет.	Лабораторные работы 5-6	Модуль 2 0÷6 за каждую ЛР «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4-5 «Отлично» - 6
	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 3 лекционных занятий, 3 практических и 3 лабораторных работы. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 14. За выполненные и защищенные практические и лабораторные занятия обучающийся получает максимум 36 балла. Общее максимальное количество баллов за модуль 1 составляет 50 баллов.

Вопросы для контрольной работы (ПК-1, ПК-2):

1. Основные нормативно-правовые акты.
2. Анализ основных руководящих документов по созданию безопасного ПО.
3. Анализ угроз безопасности ПО.
4. Анализ рисков безопасности ПО.
5. Отечественные и зарубежные стандарты в области разработки безопасного ПО.
6. Обеспечение безопасной разработки на фазе формирования требований к ПО.
7. Обеспечение безопасной разработки на фазе проектирования ПО.
8. Обеспечение безопасной разработки на фазе реализации ПО.

Практическое занятие №1. Алгоритмы шифрования данных.

Контрольные вопросы (ПК-1, ПК-2):

1. Понятие ассиметричных алгоритмов шифрования
2. Поясните суть работы Алгоритма RSA
3. В чем особенности шифрования/дешифрования изображений?
4. В чем особенности шифрования/дешифрования произвольных файлов?
5. В чем особенности защищенной передачи файлов по сети?
6. В чем особенности защищенной защищенного обмена сообщениями по сети?
7. В чем особенности шифрования/дешифрования чисел?
8. В чем особенности генерации ключей?
9. В чем особенности работы с текстом произвольной длины?

Практическое занятие №2. Защита от копирования.

Контрольные вопросы (ПК-1, ПК-2):

1. Что может использоваться в качестве анализируемых характеристик компьютера?
2. Что такое API-функции?
3. Что такое Реестр Windows?
4. Приведите примеры процедур и функций, определяющих параметры компьютера
5. Как определить версию операционной системы?
6. Как определить имя компьютера?
7. Как определить имя пользователя?

8. Как определить частоту процессора?

Практическое занятие №3. Защита от побочного электромагнитного излучения и наводок виды шифров.

Контрольные вопросы (ПК-1, ПК-2):

1. Что такое побочные излучения?
2. Что такое перехват ПЭМИН?
3. Как выполняется Защита от побочных излучений и наводок?
4. Какие есть два основных метода защиты?
5. Поясните активный метод защиты компьютерной информации от утечки по ПЭМИН.
6. Поясните пассивный метод защиты компьютерной информации от утечки по ПЭМИН.

Лабораторная работа №1. Методы поиска и сбора информации. Методика устранения компьютерной информации.

Контрольные вопросы (ПК-1, ПК-2):

1. Что такое сбор первичной базы данных?
2. Что такое индексация базы данных?
3. Что такое рафинирование результирующего списка?
4. Какие поисковые указатели являются в России наиболее крупными и популярными?
5. Приведите примеры приёмов поиска информации с помощью поисковой машины.
6. Приведите примеры устранения и восстановления информации на различных носителях
7. Приведите примеры методов восстановления файлов
8. Поясните предназначение термина Stellar Phoenix
9. Поясните предназначение термина UndeletePlus

Лабораторная работа №2. Уязвимости Windows. Защита от копирования переносных носителей

Контрольные вопросы (ПК-1, ПК-2):

1. Какие известны уязвимости Windows?
2. Каким образом происходит обнаружение уязвимостей?
3. Приведите примеры описания уязвимостей.
4. Каким образом происходит устранение уязвимостей?
5. Как происходит закрытие уязвимостей в Windows?
6. Как определить уязвимости в Windows?
7. Какой уязвимостью пользуются злоумышленники для заражения компьютеров?
8. Как происходит защита от копирования переносных носителей?
9. Приведите примеры: основные функции средств защиты от копирования?
10. Поясните основные методы защиты от копирования и криптографические методы
11. Поясните методы привязки к идентификатору
12. Поясните термин: Современные электронные ключи

Лабораторная работа №3. Модели распространения программного обеспечения.

Контрольные вопросы (ПК-1, ПК-2):

1. Что такое бесплатные программы (Freeware)?
2. Что значит почти бесплатные программы?

3. Что значит программы, показывающие рекламу?
4. Что значит коммерческие программы (Commercial)?
5. Что такое системное программное обеспечение?
6. Что такое прикладное программное обеспечение?
7. Что такое почти работоспособные программы?
8. Что такое условно бесплатные продукты.

Модуль 2 (50 баллов):

Модуль содержит 3 лекционных занятий, 3 практических и 3 лабораторных работы. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 14. За выполненные и защищенные практические и лабораторные занятия обучающийся получает максимум 36 балла. Общее максимальное количество баллов за модуль 1 составляет 50 баллов.

Вопросы для контрольной работы (ПК-1, ПК-2):

1. Меры по разработке безопасного ПО.
2. Исследование программ статическим методом. Возможные уязвимости парольной защиты программ.
3. Исследование программ статическим методом. Защита программ от исследования статическим методом.
4. Исследование программ динамическим методом. Изучение упакованных программ с помощью отладчика OllyDbg.
5. Обеспечение безопасной разработки на фазе тестирования ПО.
6. Обеспечение безопасной разработки на фазах выпуска и поддержки ПО.
7. Инструментальные средства разработки безопасных программ.
8. Инструментальные средства для безопасной разработки в среде Windows.

Практическое занятие №4. Виды шифров. Алгоритмы распределения ключей

Контрольные вопросы (ПК-1, ПК-2):

1. Поясните понятие криптографии.
2. Постройте обобщенную схему криптосистемы.
3. Что такое шифры перестановки?
4. Что такое шифрование с помощью магических квадратов?
5. Что такое шифры замены?
6. Что означает система шифрования Цезаря? Таблица подстановки шифра Цезаря.
7. Что означает Квадрат Вижинера для русского языка?
8. Поясните алгоритмы распределения ключей

Практическое занятие №5. Симметричные алгоритмы.

Контрольные вопросы (ПК-1, ПК-2):

1. Что такое симметричные криптосистемы?
2. Постройте общую схему симметричного шифрования
3. Характерная особенность симметричных блочных алгоритмов?
4. Опишите алгоритм для симметричного шифрования DES.
5. Опишите отечественный стандарт на шифрование данных.
6. Абсолютный и относительный адрес ячейки (ссылки) ГОСТ 28147-89.
7. Какой алгоритм используется в процессе шифрования?

Практическое занятие №6. Асимметричные алгоритмы.

Контрольные вопросы (ПК-1, ПК-2):

1. Что такое асимметричные алгоритмы шифрования.
2. Что такое алгоритмы шифрования с открытым ключом?
3. Что такое алгоритм шифрования с открытым ключом RSA?
4. Что такое согласование ключа?
5. Опишите алгоритм RSA.
6. Опишите алгоритм Диффи-Хеллмана.

Лабораторная работа №4. Аппаратные ключи защиты. Количественная оценка стойкости парольной защиты.

Контрольные вопросы (ПК-1, ПК-2):

1. Что такое аппаратные ключи защиты?
2. Что такое электронный ключ?
3. Поясните термин современные электронные ключи.
4. Что значит HASP?
5. Что значит eToken?
6. Что значит SecretDisk?
7. Что значит аппаратно-программные средства защиты?
8. Поясните идею обхода защиты
9. Что значит дизассемблирование?
10. Что значит декомпиляция?
11. Поясните идею количественной оценки стойкости парольной защиты

Лабораторная работа №5. Вредоносное программное обеспечение. Безопасная работа в Интернет.

Контрольные вопросы (ПК-1, ПК-2):

1. Что называется вредоносной программой?
2. Что такое компьютерный вирус? Признаки заражения.
3. Схема работы компьютерных вирусов.
4. Что значит безопасная работа в Интернет?
5. Какие данные банковских карт интересуют Злоумышленников?

Лабораторная работа №6. Обеспечение безопасности локальной сети. Настройка параметров безопасности браузера.

Контрольные вопросы (ПК-1, ПК-2):

1. Какие уязвимости ОС Windows были устранены в данной практической работе, какими способами?
2. Для чего используется утилита Netstat?
3. Перечислите, какие утилиты вошли в состав программы NetStat Agent?
4. Для чего используется каждая из утилит?
5. Для чего используется программа Nmap? TCPView?

1.3.2 Вопросы, выносимые на экзамен по дисциплине «Разработка безопасного программного обеспечения» (ПК-1, ПК-2) (промежуточная аттестация):

1. Системы кодирования. Позиционная система кодирования.
2. Понятие безопасной разработки ПО.
3. Модель безопасной разработки Cisco
4. Модель безопасной разработки Microsoft.
5. ГОСТ Р 56939-2016
6. Понятие проектирования ИС.
7. Понятие информационной технологии.
8. Компоненты технологии проектирования ИС.
9. Формирование требований безопасности к ПО.
10. Определение минимальных приемлемых уровней безопасности.
11. Определение шкалы ошибок и их влияния на безопасность.
12. Проведение оценки рисков безопасности.
13. Проектирование процессов защиты данных: понятие «угрозы», «виды угроз» безопасности хранимой информации.
14. Механизмы защиты информации. Способы и методы защиты данных.
15. Виды паролей.
16. Виды вредительских программ.
17. Виды вирусов
18. Проверка спецификаций разработки на соответствие функциональным спецификациям.
19. Анализ возможных плоскостей атак на ПО и противодействие им.
20. Анализ кода: понятие и назначение.
21. Анализ кода: инструментальные средства анализа кода.
22. Статический анализ кода: понятие, назначение, сходства и различия по сравнению с динамическим анализом.
23. Динамический анализ кода: понятие, назначение, сходства и различия по сравнению со статическим анализом.
24. Моделирование угроз.
25. Формирование и утверждение списка разрешенных инструментальных средств разработки, а также используемых стандартов.
26. Выявление устаревших или опасных библиотечных функций.
27. Статический анализ кода до компиляции.
28. Динамический анализ кода.
29. Фаззинг-тестирование.
30. Тестирование на изменение плоскости атак.
31. Планирование реагирования на инциденты с ПО.
32. Проведение окончательного обзора безопасности ПО.
33. Сертификация ПО и создание архива документации по проекту.
34. Реагирование на инциденты и выпуск обновлений безопасности.
35. Инструментальные средства для безопасной разработки в среде Windows

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 обучающимися 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 обучающимися по блокам модулей, показаны в Таблице 1.

Таблица 1 - Распределение баллов по модулям дисциплины «Разработка безопасного программного обеспечения»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок
Модуль 1	50	14	36
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: Разработка безопасного программного обеспечения		
Билет №1 1. Механизмы защиты информации. Способы и методы защиты данных. 2. Проведение окончательного обзора безопасности ПО. Кандидат технических наук _____ Швидченко С.А. «___» _____ 20__ г.		

4 Тестовые задания по дисциплине «Разработка безопасного программного обеспечения»

Тестовые задания позволяют оценить уровень сформированности 2-х компетенций ПК-1, ПК-2.

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

Количество заданий по каждой компетенции равно 20. Всего 40 заданий.

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

ПК-2. Администрирование программно-аппаратных средств защиты информации в компьютерных сетях.

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

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

№ задания	Тексты заданий
1	Выберите все безопасные типы протоколов: 1. SMTP/IMAP 2. SSL/TLS 3. HTTP 4. HTTPS 5. FTP 6. SFTP
2	Что такое SAST? 1. это процесс, который позволяет выявлять схожесть с известными типами уязвимостей, с конкретным шаблоном, структурой или правилом. 2. это процесс тестирования, при котором применяются техники статического анализа для поиска ошибок и потенциальных проблем безопасности. 3. это процесс, который осуществляет анализ основных компонентов программы с целью выявления потенциальных уязвимостей, таких как небезопасное хранение и передача данных.
3	Что происходит, если браузер не может подтвердить подлинность сертификата? 1. Соединение продолжается без изменений. 2. Браузер выдаёт предупреждение о незащищённом соединении. 3. Сертификат автоматически обновляется. 4. Браузер игнорирует сертификат и продолжает соединение.
4	Какие ошибки могут сделать сертификат невалидным? 1. Отзыв сертификата удостоверяющим центром. 2. Срок действия сертификата истек. 3. Несовпадение CN с доменным именем. 4. Ошибки в данных сертификата. 5. Все вышеперечисленное.

№ задания	Тексты заданий
5	Какова основная задача, которую решает использование HTTPS? 1. Ускорить загрузку страниц. 2. Обеспечить конфиденциальность и безопасность передаваемых данных. 3. Уменьшить объем трафика. 4. Увеличить количество отображаемых страниц.
6	Какие меры безопасности следует применять для защиты от XSS-атак? 1. Экранирование выводимых данных. 2. Валидация и фильтрация входных данных. 3. Регулярное обновление программного обеспечения. 4. Использование HTTP-Only и Secure cookie. 5. Все перечисленное.
7	Какой этап обеспечения безопасности включает анализ уязвимостей программного обеспечения? 1. анализ требований 2. тестирование безопасности 3. разработка безопасных архитектурных решений 4. тестирование производительности
8	К какому методу безопасного кодирования относится использование SSL/TLS для шифрования данных при передаче? 1. Валидация данных 2. Разграничение доступа 3. Шифрование канала связи 4. Принцип наименьших привилегий
9	Какие основные языки поддерживаются инструментами SAST? 1. C/C++, Java, PHP, .NET 2. SQL 3. HTML 4. Python, JavaScript, PHP
10	Какой тип тестирования ПО основан на спецификации и требованиях? 1. тестирование безопасности 2. нагрузочное тестирование 3. функциональное тестирование 4. модульное тестирование

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

Инструкция: Прочитайте текст и установите соответствие.

№ задания	Тексты заданий
11	Установите соответствие между недостатком SAST и его описанием: 1. Ложные срабатывания 2. Зависимость от языка 3. Уязвимые зависимости 4. Отсутствие анализа бизнес-логики А) даже лучшие анализаторы иногда выдают около 15% ложных сигналов. Б) анализатор работает только с собственным кодом приложения и не замечает уязвимости в сторонних компонентах. В) создание нового языка для SAST аналогично созданию нового продукта. Г) невозможность оценки соответствия реализации требований бизнесу.
12	Установите правильное соответствие между преимуществами SAST и их описаниями: 1. Обнаружение уязвимостей на ранней стадии 2. Высокая степень покрытия 3. Легко использовать 4. Безопасное использование А) предоставляет полное покрытие всех элементов исходного кода, минимизирует пропуски потенциальных угроз Б) нет риска нанести ущерб приложению, поскольку выполняется лишь анализ исходного кода В) простая настройка и автоматическое выполнение тестов обеспечивают быструю проверку

№ задания	Тексты заданий
	безопасности Г) можно интегрировать в процесс CI/CD и регулярно проверять каждую версию приложения
13	Установите соответствие между понятиями уязвимостей системы обеспечения безопасности ПО и их определениями: 1. Неправильная проверка ввода – 2. Переполнение буфера – 3. Условия состязания – 4. Уязвимости механизмов защиты – А) явление, возникающее, когда два различных процесса (в тех же или различных приложениях) записывают в один файл, и нет никакого способа знать, какой запишет сначала, а который перезаписал данные, уже записанные другим. Б) явление, предсказуемости формата идентификатора учетной записи (в 64% систем). Зная несколько существующих в системе идентификаторов, злоумышленник может вычислить механизм их формирования и подобрать нужный. В) явление, возникающее, когда компьютерная программа записывает данные за пределами области памяти, используемой для временного хранения данных при их вводе или выводе. Г) это вид уязвимости в программном обеспечении, который может использоваться в качестве компьютерной программы, фрагмента программного кода или последовательности команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему.
14	Установите соответствие между видами тестирования и их определениями: 1. Позитивное 2. Ручное 3. Автоматизированное 4. Негативное А) Проверка ведется в отношении программы, работающей в обычном, то есть нормальном, режиме. Другими словами, акцент делается на том, как исполняются стандартные функции продукта. Б) В этом случае проверяется работа программы в нештатной ситуации. Она может быть вызвана некорректными действиями пользователя, внутренним или внешним сбоем, другими причинами. В) Осуществляется, что вполне логично, вручную. Тестировщик фактически выступает обычным пользователем и самостоятельно проверяет соответствие программы заявленным требованиям. Г) Выполняется с применением широкого спектра специальных инструментов, работающих в автоматическом режиме, то есть независимо от тестировщика.

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

Инструкция: Прочитайте текст и установите правильную последовательность.

№ задания	Тексты заданий
15	Расположите подвиды функционального тестирования в порядке получения готового ПО: 1. End-to-End-тестирование 2. Интеграционное 3. Unit-тестирование 4. Приемочное
16	Расположите активность хакерских атак на объекты: от менее значимых к самым популярным вариантам: 1. Внутренний периметр 2. WEB-приложения 3. Внешний периметр 4. WI-FI сети 5. Мобильные приложения 6. Сотрудники (социальная инженерия)
17	Расположите этапы процесса приёмочных испытаний в правильном порядке: 1. объективная оценка 2. разработка тест-кейсов 3. формирование плана тестирования 4. анализ требований

№ задания	Тексты заданий
	5. проведение тестирования

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

Инструкция: Прочитайте текст и запишите обоснованный ответ.

№ задания	Тексты заданий
18	Интенсивное использование почти готовой версии продукта (как правило, программного или аппаратного обеспечения) с целью выявления максимального числа ошибок в его работе для их последующего устранения перед окончательным выходом продукта на рынок, к массовому потребителю это _____ - _____.
19	Защита от SQL-инъекций должна стать приоритетом любого разработчика или специалиста по кибербезопасности. Даже небольшие упущения в защите могут привести к серьезным последствиям, таким как утечка _____ клиентов.
20	За совершение преступлений, связанных с незаконным доступом к компьютерной информации, предусмотрена уголовная ответственность по статье 272 Уголовного кодекса Российской Федерации « _____ »

Система оценивания выполнения тестовых заданий по компетенции ПК-2.

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.

ПК-1. Администрирование подсистем защиты информации в операционных системах.

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

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

№ задания	Тексты заданий
1	Структурно выделенное подразделение органа исполнительной власти или субъекта хозяйствования, которое обеспечивает организацию и проведение работ по стандартизации в пределах установленной компетенции - это... 1. технический комитет по стандартизации. 2. орган государственного надзора за стандартами. 3. служба стандартизации. 4. испытательная лаборатория.
2	Документ, устанавливающий технические требования, которым должна удовлетворять продукция или услуга, а также процедуры, с помощью которых можно установить, соблюдены ли данные требования - это... 1. национальный стандарт. 2. технические условия. 3. сертификат. 4. рекомендации по стандартизации.
3	Европейские стандарты разрабатывает (ют)... 1. национальные организации стран ЕС. 2. ведомственные организации. 3. региональные организации. 4. европейский комитет по стандартизации.
4	Нормативный документ, который утверждается межгосударственной организацией по стандартизации - 1. международный стандарт. 2. региональный стандарт. 3. межгосударственный стандарт. 4. национальный стандарт.
5	Какие из перечисленных ниже утверждений являются неверными применительно к основаниям ограничения доступа к информации в Российской Федерации? 1. Ограничение доступа к информации установлено федеральным законом в целях защиты основ конституционного строя. 2. Доступ к информации ограничивается для повышения экономического роста и развития предпринимательства. 3. Федеральный закон разрешает ограничить доступ к информации для защиты нравственности, здоровья, прав и законных интересов других лиц. 4. Целью ограничения доступа к информации может быть поддержка малого бизнеса и фермерства. 5. Информация может быть закрыта в интересах национальной обороны и безопасности государства.
6	Владелец сайта и (или) страницы сайта в сети "Интернет", и (или) информационной системы, и (или) программы для ЭВМ, которые используются для обработки и распространения новостной информации в сети "Интернет" на государственном языке РФ обязаны соблюдать требования: 1. проверять достоверность распространяемых общественно значимых сведений до их распространения; 2. не размещать на новостном агрегаторе адреса электронной почты для направления им юридически значимых сообщений, а также свои фамилию и инициалы (для физического лица) или наименование (для юридического лица); 3. не допускать распространение новостной информации с целью опорочить гражданина или отдельные категории граждан; 4. бессрочно хранить распространенную ими новостную информацию, сведения об источнике ее получения, а также сведения о сроках ее распространения; 5. соблюдать права и законные интересы граждан и организаций, в том числе честь, достоинство и деловую репутацию граждан, деловую репутацию организаций.
7	Государственное регулирование в сфере применения информационных технологий (ИТ) предусматривает:

№ задания	Тексты заданий
	1. регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением ИТ (информатизации), на основании принципов, установленных настоящим Федеральным законом; 2. принуждение граждан и организаций к обязательному переходу на бумажный документооборот и отказ от электронных сервисов; 3. запрет гражданам и организациям пользоваться иностранными технологиями и программным обеспечением; 4. развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем.
8	Цифровая подпись предназначена для аутентификации лица, подписавшего электронное сообщение. Кроме того, использование ЭЦП предоставляет возможность обеспечить следующие свойства при передаче в системе подписанного сообщения: 1. повышение пропускной способности сетевых каналов связи; 2. осуществление контроля целостности передаваемого подписанного сообщения; 3. создание резервных копий всех полученных сообщений на удалённом сервере; 4. возможность автоматической расшифровки зашифрованных файлов; 5. доказательное подтверждение авторства лица, подписавшего сообщение; 6. защита сообщения от возможной подделки.
9	Неквалифицированной электронной подписью является электронная подпись, которая: 1. получена в результате криптографического преобразования информации с использованием ключа электронной подписи; 2. создана посредством простого рукописного рисунка на экране планшета; 3. формируется случайным набором символов при каждом новом сообщении; 4. позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания; 5. использует уникальный отпечаток пальца владельца устройства; 6. позволяет определить лицо, подписавшее электронный документ; 7. создается с использованием средств электронной подписи.
10	Носители персональных данных могут содержать информацию, представленную в следующих видах: 1. акустическая (речевая) информация; 2. информация, обрабатываемая в виде оптических сигналов; 3. информация, представленная в виде текста и изображений; 4. информация, обрабатываемая в виде электрических сигналов; 5. информация, представленная в виде бит, байт, файлов; 6. Все выше перечисленное.

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

Инструкция: Прочитайте текст и установите соответствие.

№ задания	Тексты заданий
11	Установите соответствие между типами протоколов TCP/IP и их уязвимостями: 1. FTP - протокол передачи файлов по сети 2. UDP - протокол передачи данных без установления соединения 3. TCP - протокол управления передачей 4. SMTP - протокол обеспечения сервиса доставки сообщений по электронной почте 5. DNS - протокол установления соответствия мнемонических имен и сетевых адресов А) Отсутствие поддержки аутентификации заголовков сообщений Б) Отсутствие механизма проверки корректности заполнения служебных заголовков пакета В) Наличие двух открытых портов Г) Отсутствие средств проверки аутентификации полученных данных от источника Д) Отсутствие механизма предотвращения перегрузок буфера
12	Установите соответствие между типами атаки и последствиями реализации угроз: 1. Анализ сетевого трафика 2. Удаленный запуск приложений 3. Внедрение ложного объекта сети 4. Навязывание ложного маршрута

№ задания	Тексты заданий
	А) Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей Б) Несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных В) Скрытое управление системой, нарушение конфиденциальности, целостности, доступности информации Г) Перехват и просмотр трафика. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
13	Установите соответствие между элементами структуры системы сертификации и функциями данных органов: 1. Национальный орган по сертификации 2. Центральный орган по сертификации 3. Испытательные лаборатории 4. Заявители и изготовители продукции и услуги А) осуществляют формирование заявок на проведение сертификации. Б) осуществляет свою деятельность, в соответствии с законом «О сертификации товаров и услуг» и Правилами Госстандарта РФ В) осуществляет свою деятельность на основе действующего законодательства РФ. Г) осуществляет испытания конкретной продукции или конкретные виды испытаний и выдает протоколы испытаний.
14	Установите соответствие между видами классификации и их определениями: 1. Селекция – 2. Симплификация – 3. Типизация – 4. Унификация – А) экономически обоснованное приведение изделий к единообразию на основе установления рационального числа разновидностей типа изделий и документации. Б) деятельность, заключающаяся в отборе конкретных объектов, которые признаются целесообразными для дальнейшего производства и применения в общественном производстве. В) метод, заключающийся в установлении типовых (образцовых) объектов – конструкций, технологических правил, форм документации. Г) деятельность, заключающаяся в определении таких конкретных объектов, которые признаются на основании анализа их перспективности нецелесообразными для дальнейшего производства, т. е. ограничение числа объектов.

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

Инструкция: Прочитайте текст и установите правильную последовательность.

№ задания	Тексты заданий
15	Расположите примеры стандартов по понижению уровня значимости: 1. ГОСТ Р 59711-2022 «Организация деятельности по управления компьютерными инцидентами» 2. ISO/IEC 25010 «Системная и программная инженерия 3. ГОСТ 34.10-2018 «Информационная технология. Криптографическая защита информации» 4. ГОСТ Р ИСО/МЭК 25051-2017 «Информационные технологии (ИТ)»
16	Установите нормативные документы в правильном хронологическом порядке: 1. Федеральный закон «О стандартизации в Российской Федерации» 2. Декрет «О введении Международной метрической системы мер и весов» 3. «Регламент об управлении Адмиралтейства и верфи» 4. Постановление «О стандартизации экспортируемых товаров»
17	Расположите документы, устанавливающие порядок проведения мероприятий с целью защиты данных в порядке их важности: 1. Распоряжение о правилах хранения электронных и бумажных носителей ценных сведений, определения порядка допуска к ним. 2. Утвержденный список лиц с доступом к информации, имеющей стратегическое значение.

№ задания	Тексты заданий
	3. Положение о защите персональных, секретных, конфиденциальных сведений. 4. Должностные инструкции специалистов, ответственных за программное обеспечение, работу технических средств, контролирующих доступность сведений. 5. Правила проведения процедуры идентификации пользователей.

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

Инструкция: Прочитайте текст и запишите обоснованный ответ.

№ задания	Тексты заданий
18	Технический прием, включающий преобразование объектного кода в исходный текст в целях изучения структуры и кодирования программы для ЭВМ – это _____.
19	Средства криптографической защиты информации (СКЗИ) и их опытные образцы подлежат _____ с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов (условных наименований) и регистрационных номеров СКЗИ и их опытных образцов определяет ФСБ России.
20	Процедура подтверждения соответствия, посредством которой независимая от изготовителя (продавца, исполнителя) и потребителя (покупателя) организация удостоверяет в письменной форме, что продукция соответствует установленным требованиям – это _____.

Система оценивания выполнения тестовых заданий по компетенции ПК-1.

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 *«Разработка безопасного программного обеспечения»* для обучающихся очной формы обучения

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 занятий, 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.