Федеральное государственное бюджетное образовательное учреждение высшего образования

РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА и ГОСУДАРСТВЕННОЙ СЛУЖБЫ при ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕВЕРО-ЗАПАДНЫЙ ИНСТИТУТ УПРАВЛЕНИЯ

Факультет среднего профессионального образования

УТВЕРЖДЕНА
решением цикловой (методической) комиссии общепрофессиональных дисциплин и по профессиональным модулям специальности 09.02.07 Информационные системы и программирование
Протокол от 31.10.2025 № 2

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МДК.02.06. Безопасность программного обеспечения

Специальность – 09.02.11 Разработка и управление программным обеспечением

Профиль – на базе основного общего образования

Квалификация – программист

Форма обучения – очная

Год набора – 2026

Санкт-Петербург 2025 год

Автор-составитель: Мультан Маргарита Александровна, преподаватель ФСПО СЗИУ РАНХиГС.

СОДЕРЖАНИЕ

1 Общие положения

1.1 Область применения программы

Рабочая программа учебной дисциплины «Безопасность программного обеспечения» является частью профессиональной подготовки обучающихся направления подготовки 09.02.11 «Разработка и управление программным обеспечением».

1.2 Место дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина «Безопасность программного обеспечения» является частью профессиональной подготовки и входит в профессиональный цикл дисциплин.

Для успешного освоения дисциплины предполагается освоение таких предшествующих дисциплин, как «Информатика», «Математический аппарат в отрасли информационных технологий», «Основы работы с информацией», «Основы информационной безопасности», «Разработка программных модулей», «Операционные системы и среды», «Компьютерные сети». Полученные в результате освоения дисциплины знания, умения и практические навыки необходимы и будут полезны для последующего изучения дисциплины «Технологии безопасности мобильных платформ».

Дисциплина изучается на 3 курсе в 6 семестре.

1.3 Цели и задачи учебной дисциплины

Цель дисциплины «Безопасность программного обеспечения»: формирование представлений о существующих угрозах и уязвимостях ПО и ОС, разработка надежного и защищенного программного обеспечения и его отдельных модулей на современных языках программирования для различных операционных систем и устройств; формирование подхода к созданию защищенных приложений, который включает в себя предупреждение, обнаружение и устранение уязвимостей на всех этапах жизненного цикла разработки программного обеспечения.

1.4 Планируемые результаты обучения по дисциплине

Перечень общих компетенций

Код и наименование компетенции	Умения	Знания
ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	- распознавать задачу и/или проблему в профессиональном и/или социальном контексте, анализировать и выделять её составные части; - определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы;	- актуальный профессиональный и социальный контекст, в котором приходится работать и жить; - структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях; - основные источники информации и ресурсы для решения задач и/или

Код и наименование компетенции	Умения	Знания
	- выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; - владеть актуальными методами работы в профессиональной и смежных сферах; - оценивать результат и последствия своих действий (самостоятельно или с помощью наставника);	проблем в профессиональном и/или социальном контексте; - методы работы в профессиональной и смежных сферах; - порядок оценки результатов решения задач профессиональной деятельности;
ОК 02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	- определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации; - выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять результаты поиска; - оценивать практическую значимость результатов поиска; - применять средства информационных технологий для решения профессиональных задач; - использовать современное программное обеспечение в профессиональной деятельности; - использовать различные цифровые средства для решения профессиональных задач;	- номенклатура информационных источников, применяемых в профессиональной деятельности; - приемы структурирования информации; - формат оформления результатов поиска информации; - современные средства и устройства информатизации, порядок их применения и программное обеспечение в профессиональной деятельности, в том числе цифровые средства;
ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	- определять актуальность нормативно-правовой документации в профессиональной деятельности; - применять современную научную профессиональную терминологию; - определять и выстраивать траектории профессионального развития и самообразования; - выявлять достоинства и недостатки коммерческой идеи; - определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности, выявлять источники финансирования; - презентовать идеи открытия собственного дела в профессиональной деятельности; - определять источники достоверной правовой информации; - составлять различные правовые документы;	- содержание актуальной нормативно-правовой документации; - современная научная и профессиональная терминология; - возможные траектории профессионального развития и самообразования; - основы предпринимательской деятельности, правовой и финансовой грамотности; - правила разработки презентации; - основные этапы разработки и реализации проекта;

Код и наименование компетенции	Умения	Знания
	- находить интересные проектные идеи, грамотно их формулировать и документировать; - оценивать жизнеспособность проектной идеи, составлять план проекта;	
ОК 04 Эффективно взаимодействовать и работать в коллективе и команде	- организовывать работу коллектива и команды; - взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности;	- психологические основы деятельности коллектива; - психологические особенности личности;
ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	- грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке; - проявлять толерантность в рабочем коллективе;	- правила оформления документов; - правила построения устных сообщений; - особенности социального и культурного контекста;
ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	- проявлять гражданско-патриотическую позицию; - демонстрировать осознанное поведение; - описывать значимость своей специальности; - применять стандарты антикоррупционного поведения;	- сущность гражданско-патриотической позиции; - традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений; - значимость профессиональной деятельности по специальности; - стандарты антикоррупционного поведения и последствия его нарушения;
ОК 07 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	- соблюдать нормы экологической безопасности; - определять направления ресурсосбережения в рамках профессиональной деятельности по специальности; - организовывать профессиональную деятельность с соблюдением принципов бережливого производства; - организовывать профессиональную деятельность с учетом знаний об изменении климатических условий региона; - эффективно действовать в чрезвычайных ситуациях;	- правила экологической безопасности при ведении профессиональной деятельности; - основные ресурсы, задействованные в профессиональной деятельности; - пути обеспечения ресурсосбережения; - принципы бережливого производства; - основные направления изменения климатических условий региона; - правила поведения в чрезвычайных ситуациях;

Код и наименование компетенции	Умения	Знания
ОК 08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня	- использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; - применять рациональные приемы двигательных функций в профессиональной деятельности; - пользоваться средствами профилактики перенапряжения, характерными для данной специальности;	- роль физической культуры в общекультурном, профессиональном и социальном развитии человека; - основы здорового образа жизни; - условия профессиональной деятельности и зоны риска физического здоровья для специальности; - средства профилактики перенапряжения;
ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках	- понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; - участвовать в диалогах на знакомые общие и профессиональные темы; - строить простые высказывания о себе и о своей профессиональной деятельности; - кратко обосновывать и объяснять свои действия (текущие и планируемые); - писать простые связные сообщения на знакомые или интересующие профессиональные темы;	- правила построения простых и сложных предложений на профессиональные темы; - основные общеупотребительные глаголы (бытовая и профессиональная лексика); - лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; - особенности произношения, правила чтения текстов профессиональной направленности;

Перечень профессиональных компетенций

Код и наименование компетенции	Навыки	Умения	Знания
ПК 2.1 Проектировать модули программного обеспечения	- проектирования модулей ПО с учетом требований заказчика; - создания архитектурных диаграмм и спецификаций модулей; - определения интерфейсов и взаимодействия модулей в системе;	- проектировать модули, соответствующие бизнес-задачам; - создавать архитектурные диаграммы и документацию; - определять структуру и интерфейсы модулей; - анализировать требования к модулю и определять его функциональность; - проектировать архитектуру модуля, включая выбор подходящих паттернов проектирования и структуры данных; - создавать диаграммы классов, последовательностей и прочих диаграмм для	- основные принципы проектирования модулей программного обеспечения; - языки программирования и технологии для реализации модулей; - паттерны проектирования и структуры данных для создания эффективных и масштабируемых модулей; - методы анализа требований и способов определения функциональности модуля;

Код и наименование компетенции	Навыки	Умения	Знания
		визуализации проектируемого модуля; - выбирать подходящие языки программирования и технологии для реализации модуля; - проектировать интерфейсы программного обеспечения для взаимодействия с другими модулями и системами; - учитывать требования к масштабируемости, производительности и безопасности при проектировании модуля; - проводить анализ и оптимизацию проектируемого модуля для повышения его эффективности и качества;	- принципы создания интерфейсов для взаимодействия с другими модулями и системами; - принципы обеспечения безопасности, производительности и масштабируемости при проектировании модулей; - методы анализа и оптимизации проектируемых модулей для повышения их эффективности и качества;
ПК 2.2 Разрабатывать модули программного обеспечения	- создание модулей программного обеспечения на различных языках программирования; - отладки и тестирования разработанных модулей; - применение структурного и объектно-ориентированного программирования; - оптимизации кода и алгоритмов программных модулей для увеличения производительности; - мониторинга и анализа производительности приложений;	- разрабатывать модули программного обеспечения с использованием различных языков программирования и технологий; - применять паттерны проектирования и структуры данных для создания эффективных и масштабируемых модулей; - анализировать требования и определять функциональность модуля; - создавать интерфейсы для взаимодействия с другими модулями и системами; - обеспечивать безопасность, производительность и масштабируемость при разработке модулей; - оптимизировать проектируемые модули для повышения их эффективности и качества; - работать с системой контроля версий; - улучшать производительность модулей, выявляя и устраняя узкие места; - проводить анализ и мониторинг	- язык программирования, основные конструкции, синтаксис; - паттерны проектирования; - структуры данных; - принципы создания интерфейсов для взаимодействия с другими модулями и системами, таких как REST API, SOAP; - работа с инструментальным программным обеспечением; - методы оптимизации кода и алгоритмов; - эффективные алгоритмы и структуры данных для повышения производительности; - многопоточность в программных модулях; - методы оптимизации сетевых протоколов для ускорения обмена данными; - кэширование данных; - управление памятью; - техники повышения производительности

Код и наименование компетенции	Навыки	Умения	Знания
		производительности приложений; - применять инструменты для рефакторинга и оптимизации программного кода;	программного обеспечения;
ПК 2.3 Выполнять интеграцию модулей и компонентов программного обеспечения	- интеграции программных модулей и компонентов в единое программное решение; - работы с API и веб-сервисами для взаимодействия между модулями; - работы с интеграционными платформами и инструментами обеспечения совместимости и стабильности системы;	- интегрировать модули и компоненты, обеспечивая их взаимодействие; - работать с API и устанавливать соединения между компонентами; - отслеживать и устранять конфликты и ошибки интеграции; - анализировать и определять зависимости между модулями и компонентами; - работать с различными форматами данных и протоколами передачи данных;	- общих принципов функционирования аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы; - международных стандартов локальных вычислительных сетей; - методы и подходы к интеграции модулей и компонентов; - принципы версионирования и управления изменениями при интеграции; - принципы безопасности при интеграции модулей и компонентов;
ПК 2.4 Выполнять тестирование и отладку программного обеспечения	- отладки программного обеспечения на уровне программных модулей; - тестирования программного обеспечения; - формирования тестовых сценариев; - подготовки тестовых платформ (установка операционной системы, дополнительного ПО и другого по необходимости); - оценки объема тестирования ПО с целью определения необходимых ресурсов для его выполнения; - настройки тестовой среды и аппаратных средств для выполнения	- анализировать требования к программному обеспечению и составлять планы тестирования; - создавать тестовые сценарии и тест-кейсы для проверки функциональности и соответствия требованиям; - выполнять тестирование программного обеспечения вручную и автоматизировать процесс тестирования; - анализировать результаты тестирования и документировать найденные ошибки; - разрабатывать стратегии отладки и исправлять ошибки в программном обеспечении; - выполнять модульные тесты с использованием инструментов тестирования, в том числе автоматизированного тестирования;	- принципы и методы тестирования программного обеспечения; - основы программирования и архитектуры программного обеспечения; - основы баз данных и SQL-запросов; - инструменты для автоматизации тестирования; - основы разработки и отладки программного обеспечения на разных языках программирования; - понятие дефекта программного обеспечения; - критерии качества ПО; - виды и типы тестирования ПО;

Код и наименование компетенции	Навыки	Умения	Знания
	тестирования ПО в соответствии с заданием на тестирование в пределах своей компетенции; - формирования и представления отчетности о подготовке к выполнению задания на тестирование ПО в соответствии с установленными регламентами; - выполнения тестовых процедур на тестовых данных;	- использовать системы контроля дефектов ПО; - составлять отчет о выполнении тестирования ПО;	- техники ручного тестирования; - техники автоматизированного тестирования; - жизненный цикл дефекта ПО; - принципы работы в системе контроля дефектов; - основные понятия о качестве ПО;
ПК 2.5 Осуществлять документирование программных модулей программного обеспечения	- создания технической документации для модулей; - документирования кода, API и интерфейсов; - работы со специализированным ПО по документированию программного кода;	- описывать функциональность модулей в документации; - создавать диаграммы для иллюстрации работы модулей; - программировать с использованием комментариев для документирования кода; - использовать специальные метки/теги для отметки важных частей кода в документации; - вести журнал изменений и фиксировать обновления программных модулей; - разбивать модули на логические блоки и описывать каждый блок отдельно; - включать в документацию особенности модулей, такие как ограничения, уязвимости или оптимальные настройки; - проводить регулярное обновление документации при изменении модулей или добавлении нового функционала;	- стандарты технической документации; - принципы документирования программного обеспечения; - инструменты для создания технической документации и комментирования кода;

В результате освоения учебной дисциплины студент должен:

иметь практический опыт	- чтения и составления технической документации; - разработки кода программного продукта на основе готовой спецификации; - использования инструментальных средств на этапе отладки программного обеспечения; - анализа требований к безопасности программного обеспечения и создания спецификаций безопасности; - проведения статического и динамического тестирования кода на наличие уязвимостей; - настройки и аудита механизмов аутентификации и авторизации в приложениях; - применения криптографических методов для обеспечения конфиденциальности данных (хеширование, шифрование, цифровые подписи); - анализа и корректной обработки инцидентов безопасности, связанных с уязвимостями в ПО; - разработки безопасного кода на одном из языков программирования (C/C++, Java, C#, Python) с учетом основных принципов безопасности;
уметь	- находить на государственных порталах нормативные документы для разработки программного обеспечения; - выбирать инструменты и методы для разработки программного обеспечения; - классифицировать угрозы и атаки на программное обеспечение, используя существующие модели; - выявлять и устранять распространенные уязвимости; - применять принципы безопасного программирования (например, принцип наименьших привилегий, валидация ввода, экранирование вывода); - анализировать исходный код и исполняемые файлы на предмет наличия дефектов безопасности; - оценивать риски, связанные с выявленными уязвимостями, и выбирать адекватные меры устранения и защиты; - разрабатывать и документировать тест-кейсы для проверки безопасности приложения; - настраивать базовые средства защиты операционной системы и сети, влияющие на безопасность приложения (например, брандмауэры, политики доступа);
знать	- классификацию программного обеспечения; - модели жизненного цикла программного обеспечения; - модели разработки программного обеспечения; - классификацию языков программирования и сферы их применения; - инструменты разработки программного обеспечения и его отдельных модулей для различных операционных систем и устройств; - основные понятия и принципы информационной безопасности; - классификацию и механизмы реализации наиболее опасных уязвимостей программного обеспечения; - модели и методологии обеспечения безопасности на протяжении всего жизненного цикла разработки ПО; - основы криптографии: симметричное и асимметричное шифрование, хеш-функции, электронная цифровая подпись, сертификаты; - правовые и нормативные требования в области безопасности информации и защиты персональных данных; - принципы работы сетевых протоколов и связанные с ними угрозы; - методы и средства аутентификации, авторизации и управления сессиями.

2 Структура и содержание дисциплины

2.1 Объем учебной дисциплины и виды работ

Виды учебной работы	Объем учебной работы, час.
Учебная нагрузка обучающихся всего, в том числе:	88
лекции	16
практические занятия	66
курсовая работа	-
самостоятельная работа обучающихся	4
консультации	2
промежуточная аттестация	6
Форма промежуточной аттестации	Зачет с оценкой

2.2 Тематический план и содержание дисциплины

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)	Распределение часов			Формируемые компетенции	Формы текущего контроля
			Л	ПР	СРС		
1.	Тема 1. Введение в надежность и безопасность программного обеспечения	**Содержание учебного материала** 1. Виды программного обеспечения. Системное (базовое) программное обеспечение. Прикладное программное обеспечение. Программы встроенных систем. 2. Функциональная надежность программного обеспечения в информационных системах. 3. Понятие общей надежности информационной системы. 4. Отказобезопасность и кибербезопасность информационных систем. 5. Взаимосвязь функциональной и информационной безопасности критически важных систем.	2	-	-	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ПК 2.3, ПК 2.4, ПК 2.5	О,Т
2.	Тема 2. Угрозы надежности и безопасности программного обеспечения	**Содержание учебного материала** 1. Уязвимости программного обеспечения. 2. Ошибки в программном обеспечении. 3. Характерные недостатки эксплуатируемых программ. 4. Вредоносные программы. **Практические занятия:** 1. Уязвимости программного обеспечения. 2. Ошибки в программном обеспечении. 3. Характерные недостатки эксплуатируемых программ. 4. Вредоносные программы.	2	12	-	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ПК 2.3, ПК 2.4, ПК 2.5	О, ПЗ, Т.

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)	Распределение часов			Формируемые компетенции	Формы текущего контроля
			Л	ПР	СРС		
3.	Тема 3. Защитные механизмы операционных систем	**Содержание учебного материала** 1. Информационная безопасность. 2. Безопасные системы и угрозы безопасности. 3. Роль операционных систем в обеспечении информационной безопасности. 4. Идентификация и аутентификация. Общая схема процесса идентификации и аутентификации. Аутентификация с использованием паролей. Аутентификация с использованием физического объекта. Аутентификация с использованием биометрических данных. 5. Авторизация и методы разграничения доступа. Методы реализации дискреционной модели доступа. Многоуровневый доступ. 6. Дополнительные меры безопасности. Контроль повторного использования объектов. Анализ тайных каналов передачи информации. Аудит и протоколирование системы защиты. Требования надежности систем безопасности. Понятие классов безопасности. 7. Безопасность современных операционных систем. **Практические занятия:** 1. Безопасность в Windows. 2. Безопасность в UNIX.	2	8	-	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5	О, ПЗ, Т.
4.	Тема 4. Правила и этапы построения надежного программного обеспечения	**Содержание учебного материала** 1. Маршрутная карта обеспечения функциональной надежности программного обеспечения. 2. Модели надежности программного обеспечения. Исходные данные и некоторые понятия. Анализ существующих моделей надежности программного обеспечения. 3. Показатели функциональной надежности и функциональной безопасности ПО. **Практические занятия:** 1. Показатели стабильности 2. Показатели готовности к работе 3. Показатели отказоустойчивости 4. Показатели восстанавливаемости 5. Расчет функциональной надежности программ.	2	12	1	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5	О, ПЗ, Т.

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)	Распределение часов			Форми-руемые компетен-ции	Формы текущего контроля
			Л	ПР	СРС		
		6. Расчет показателей безопасности программ. 7. Показатели конфиденциальности 8. Показатели целостности 9. Показатели неопровержимости 10. Показатели отчетности 11. Показатели аутентификации 12. Показатели модульности 13. Показатели повторного использования 14. Показатели подверженности анализу 15. Показатели модифицируемости 16. Показатели тестируемости 17. Показатели адаптивности 18. Показатели установки 19. Показатели заменяемости 20. Расчет показателей долговечности программ. 21. Расчет комплексных показателей надежности программ.					
5.	Тема 5. Технологии разработки надежного программного обеспечения	**Содержание учебного материала** 1. Рекомендации по разработке спецификации требований. 2. Технология разработки архитектуры надежной программы. Классификация методов построения архитектуры надежной программы. Предупреждение ошибок. Обнаружение ошибок. Исправление ошибок. Устойчивость к ошибкам. 3. Проектирование надежного программного обеспечения и его реализация. 4. Интеграция программного обеспечения с аппаратными средствами. 5. Обеспечение надежности программного обеспечения в процессе подтверждения соответствия, эксплуатации и сопровождения. Подтверждение соответствия программного обеспечения. Эксплуатация, сопровождение и конфигурация функционально надежных программных средств. 6. Требования к функциональной надежности и архитектуре программного обеспечения критически важных систем. Спецификация требований к	2	10	-	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5	О, ПЗ, Т.

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)	Распределение часов			Форми-руемые компетен-ции	Формы текущего контроля
			Л	ПР	СРС		
		функциональной надежности ПО. Требования к архитектуре функционально надежного ПО. **Практические занятия:** 1. Разработка архитектуры надежной программы. 2. Интеграция программного обеспечения с аппаратными средствами 3. Эксплуатация, сопровождение и конфигурация функционально надежных программных средств 4. Требования к функциональной надежности и архитектуре программного обеспечения критически важных систем					
6.	Тема 6. Методы и технологии обеспечения безопасности программного обеспечения	**Содержание учебного материала** 1. Методы доказательства правильности программ. Общие положения. Предусловия и постусловия в доказательствах правильности. Правила вывода (доказательства). Применение правил вывода. Пример доказательства правильности программы для алгоритма дискретного экспоненцирования. 2. Методы создания самотестирующихся и самокорректирующихся программ. Общие положения. Области применения самотестирующихся и самокорректирующихся программ и их сочетаний. 3. Криптографические методы защиты от вредоносных программ. Методы аутентификации и обеспечения целостности программ. Методы инкрементальной криптографии. 4. Технологии защиты от вредоносных программ. Классификация вредоносных программ. Защита от вредоносных программ. 5. Технологии тестирования программного обеспечения на его защищенность. Методологические основы анализа программных средств на предмет наличия (отсутствия) недекларированных возможностей. Построение программно-аппаратных	2	10	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5	О, ПЗ, Т.

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)	Распределение часов			Форми-руемые компетен-ции	Формы текущего контроля
			Л	ПР	СРС		
		комплексов для контроля технологической безопасности программ. Методы тестирования и квалификационного тестирования программ. Фаззинг программ. 6. Методы защиты программ от несанкционированного исследования. Способы защиты программ от несанкционированного исследования. Способы встраивания защитных механизмов в программное обеспечение. Обфускация и деобфускация программ. **Практические занятия:** 1. Самотестирующиеся / самокорректирующиеся программы. 2. Криптографические методы защиты. 3. Защита от вредоносных программ. 4. Технологии тестирования программного обеспечения на его защищенность. 5. Обфускация и деобфускация программ					
7.	Тема 7. Отечественные нормативные акты, регламентирующие деятельность в области обеспечения надежности и безопасности программного обеспечения	**Содержание учебного материала** 1. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации». 2. ГОСТ Р ИСО/МЭК 15408-2013. ГОСТ Р ИСО/МЭК 18045-2013. ГОСТ Р МЭК 61508-2012. 3. Приказ ФСТЭК России от 14 марта 2014 г. 31. 4. Руководящий документ ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей». 5. Требования к средствам антивирусной защиты (информационное сообщение ФСТЭК России от 30 июля 2012 г. 240/24/3095). **Практические занятия:** 1. Основные положения Руководящего документа ФСТЭК России «Защита от несанкционированного доступа к	2	6	1	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ПК 2.1, ПК 2.3, ПК 2.4, ПК 2.5	О,ПЗ

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)	Распределение часов			Форми-руемые компетен-ции	Формы текущего контроля
			Л	ПР	СРС		
		информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей». 2. Международные организации, осуществляющие стандартизацию информационных технологий (ISO, IEEE, ITU).					
8.	Тема 8. Подтверждение соответствия надежности и безопасности программного обеспечения	**Содержание учебного материала** 1. Основные понятия в области подтверждения соответствия. 2. Натурные испытания надежности и безопасности информационных систем. 3. Методы ускорения испытаний. Два подхода к ускорению испытаний. Метод Монте-Карло. Метод значимой выборки. 4. Метод ускоренных натурных испытаний на надежность и функциональную безопасность информационных систем. Теоретические основы метода ускоренных натурных испытаний. Приложение метода к ускоренным натурным испытаниям информационной системы управления технологическими процессами. Оценка продолжительности испытаний. 5. Пример ускоренных натурных испытаний на функциональную безопасность информационной системы управления технологическим процессом. Описание объекта испытаний. Цель испытаний и критерии отказов. Алгоритмы генерации сбоев и помех. Порядок проведения испытаний. Обработка и оценка результатов испытаний. 6. Основные положения Методики испытаний качества и функциональной безопасности программного обеспечения. 7. Основные положения Методики испытаний по требованиям безопасности информации. Перечень проверок и испытаний. Контроль состава и содержания документации. Контроль исходного состояния ПО. Статический анализ исходных	2	8	-	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5	О, ПЗ, Т.

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)	Распределение часов			Форми-руемые компетен-ции	Формы текущего контроля
			Л	ПР	СРС		
		текстов программ. Динамический анализ исходных текстов программ. Контроль полноты и корректности реализации технических приемов. Обработка, анализ и оценка результатов испытаний. 8. Порядок подтверждения соответствия требованиям комплексной безопасности программного обеспечения. **Практические занятия:** 1. Контроль состава и содержания документации. 2. Контроль исходного состояния ПО. 3. Статический и динамический анализ исходных текстов программ.					
		Итого часов:	16	66	4		

2.3 Регламент распределения видов работ по дисциплине с ДОТ

Данная дисциплина реализуется с применением дистанционных образовательных технологий (ДОТ). Распределение видов учебной работы, форматов текущего контроля представлены в Таблице 2.3.

Таблица 2.3. — Распределение видов учебной работы и текущей аттестации

Вид учебной работы	**Формат проведения**
Лекционные занятия	Частично с применением ДОТ
Практические занятия	Частично с применением ДОТ
Текущий контроль	Частично с применением ДОТ
Промежуточная аттестация	Контактная аудиторная работа
Формы текущего контроля	**Формат проведения**
Тестирование	Частично с применением ДОТ
Доклады	Контактная аудиторная работа
Опрос	Контактная аудиторная работа
Практические задания	Частично с применением ДОТ

Доступ к системе дистанционных образовательных программ осуществляется каждым обучающимся самостоятельно с любого устройства на портале: https://sziu-de.ranepa.ru в соответствии с их индивидуальным паролем и логином к личному кабинету / профилю.

Текущий контроль, проводимый в системе дистанционного обучения, оцениваются как в системе дистанционного обучения, так и преподавателем вне системы.

Доступ к материалам лекций предоставляется в течение всего семестра по мере прохождения освоения программы. Доступ к каждому виду работ и количество попыток на выполнение задания предоставляется ограниченное время согласно регламенту дисциплины, опубликованному в системе дистанционного обучения. Преподаватель оценивает выполненные обучающимися работы не позднее 14 рабочих дней после окончания срока выполнения.

3 Материалы текущего контроля успеваемости и промежуточной аттестации обучающихся

3.1 Формы и методы текущего контроля успеваемости и промежуточной аттестации обучающихся

Формы текущего контроля успеваемости:

Опрос (О) позволяет выявить правильность ответа по содержанию, его последовательность, самостоятельность суждений и выводов, степень развития логического мышления.

Тестирование (Т) – задания, с вариантами ответов.

Критерии оценивания

Оценки «отлично» заслуживает студент, если он ответил правильно на 90% вопросов теста;

Оценки «хорошо» заслуживает студент, если он ответил правильно на часть вопросов 75%-90%;

Оценки «удовлетворительно» заслуживает студент, если он правильно ответил часть вопросов 50%-75%;

Оценки «неудовлетворительно» заслуживает студент, если он правильно ответил менее чем на 50% вопросов.

Практическое задание (ПЗ) используется для закрепления теоретических знаний и отработки навыков и умений, способности применять знания при решении конкретных задач. Промежуточная аттестация проходит в форме собеседования по вопросам из перечня, заранее подготовленного и предоставленного для ознакомления студентам. По результатам прохождения зачёта выставляется отметка по общеустановленной пятибалльной шкале.

Критерии оценивания форм текущей и промежуточной аттестаций:

Оценки «отлично» заслуживает студент, обнаруживший глубокое знание материала, умение свободно выполнять задания, понимающий взаимосвязь основных понятий темы;

Оценки «хорошо» заслуживает студент, обнаруживший полное знание материала; успешно выполняющий предусмотренные задания; и допустивший незначительные ошибки: неточность фактов, стилистические ошибки;

Оценки «удовлетворительно» заслуживает студент, обнаруживший знания основного материала в объеме, необходимом для дальнейшего изучения дисциплины. Справляющийся с выполнением заданий; допустивший погрешности в ответе, но обладающий необходимыми знаниями для их устранения под руководством преподавателя;

Оценки «неудовлетворительно» заслуживает студент, обнаруживший существенные пробелы в знании основного материала; не справляющийся с выполнением заданий, допустивший серьезные погрешности в ответах, нуждающийся в повторении основных разделов курса под руководством преподавателя.

Формы текущего контроля

№	Название темы	Формы текущего контроля успеваемости
1.	Тема 1. Введение в надежность и безопасность программного обеспечения	Т, О
2.	Тема 2. Угрозы надежности и безопасности программного обеспечения	Т, ПЗ, О
3.	Тема 3. Защитные механизмы операционных систем	Т, ПЗ, О
4.	Тема 4. Правила и этапы построения надежного программного обеспечения	Т, ПЗ, О
5.	Тема 5. Технологии разработки надежного программного обеспечения	Т, ПЗ, О
6.	Тема 6. Методы и технологии обеспечения безопасности программного обеспечения	Т, ПЗ, О
7.	Тема 7. Отечественные нормативные акты, регламентирующие деятельность в области обеспечения надежности и безопасности программного обеспечения	О, ПЗ
8.	Тема 8. Подтверждение соответствия надежности и безопасности программного обеспечения	Т, ПЗ, О

Примечание. В столбце «Форма текущего контроля успеваемости, промежуточной аттестации» перечисляются все используемые в учебном процессе по данной дисциплине формы контроля освоения материала. (Т – тестирование; ПЗ – практическое задание, О-опрос).

3.2 Оценочные средства текущего контроля успеваемости обучающихся.

Примеры типовых практических заданий

Практическая работа 2.4. Вредоносные программы

Содержание работы: изучение устройства, состава и кода компонентов вредоносных скриптов, запуск и отключение скриптов на виртуальной машине с целью овладения навыками нейтрализации угрозы и ее последствий, редактирование кода вредоносных скриптов для обезвреживания программы.

Практическая работа 7.2. Международные организации, осуществляющие стандартизацию информационных технологий (ISO, IEEE, ITU)

Задание: Посетите сайты ведущих международных организаций, осуществляющих стандартизацию информационных технологий (ISO, IEEE, ITU). Приведите схему, показывающую организационную структуру этих организаций. На основе найденной вами информации опишите процесс работы над стандартами в этой организации, правила согласования и принятия стандартов.

Примеры тестовых заданий

1. К какому виду программного обеспечения относятся операционные системы?

а) прикладное программное обеспечение

б) системное программное обеспечение

в) программы встроенных систем

г) инструментальное программное обеспечение

2. Вредоносная программа, способная самостоятельно распространяться по сети без участия пользователя, — это:

а) вирус

б) червь

в) троян

г) шпионское ПО

3. Какой документ описывает последовательность действий и решений на протяжении всего жизненного цикла ПО для достижения требуемой надежности?

а) модель надежности

б) маршрутная карта обеспечения функциональной надежности

в) техническое задание

г) пользовательская инструкция

4. Ключевой документ, с которого начинается разработка надежного ПО, описывающий, что должна делать система: _____.

Примеры устного опроса по теме:

Угрозы надежности и безопасности программного обеспечения

1. Какой объект в информационной системе является наиболее вероятным для воздействия? Дайте определения терминам «защищенность ПО ИС» и «уровень безопасности ПО».
2. Что подразумевается под технологической и эксплуатационной безопасностью ПО?
3. Дайте определения понятиям «объект защиты», «системное ПО», «общесистемное ПО», «специальное ПО» и «прикладное ПО».
4. Каковы основные принципы обеспечения безопасности программного обеспечения?
5. Приведите типы компьютерных атак на ИС, поражающих ПО.
6. Перечислите методы защиты современного ПО. Приведите примеры.
7. Приведите классификацию вредоносных программ, в том числе компьютерных вирусов. Опишите различные типы компьютерных вирусов в соответствии с этой классификацией.
8. Приведите примеры компьютерных вирусов, с которыми вы сталкивались. К какому типу вирусов вы их отнесете?
9. Опишите средства нейтрализации компьютерных вирусов. Приведите примеры использования антивирусных комплексов.
10. Какие существуют методы защиты программ от исследования? Приведите классификацию средств исследования программ.
11. Какие методы защиты программ от несанкционированного копирования вам известны? Охарактеризуйте кратко каждый метод.
12. Какая атака на защищенную ИС является наиболее опасной?
13. Что представляет собой программная закладка?
14. Каким образом закладка может быть внедрена в информационную систему?
15. Приведите классификацию программных закладок.
16. В чем суть работы клавиатурных шпионов?
17. Что в целом называется троянской программой?
18. В чем отличие закономерных бомб от вирусов?

19. Каковы способы внедрения программных закладок на этапе создания ПО?

20. Что такое угроза?

21. Что такое риск?

22. Что такое уязвимость?

23. Что такое недекларированные возможности (НДВ)?

24. Какие виды НДВ Вы знаете?

25. Что такое закладка?

26. Что такое SQL-инъекция?

27. Что такое переполнение буфера?

28. Чем характеризуется атака переполнения буфера?

29. Что такое DOS-атака?

30. Виды DOS-атак.

31. Что такое распределенная DOS-атака?

3.3 Оценочные средства промежуточной аттестации обучающихся

Вопросы для подготовки к зачету с оценкой

1. Определения уровней ПО, их взаимосвязь и взаимодействие.
2. Определения понятий «системное (базовое) ПО», «прикладное ПО» и «программы встроенных систем».
3. Определение понятия «функциональная надежность ПО». Объект исследований функциональной надежности ПО.
4. Понятия «функциональный отказ», сбой функционального характера и сбойная ошибка.
5. Отличия между надежностью программ и надежностью технических средств.
6. Определение понятия «общая надежность ИС». Дерево общей надежности ПО.
7. Определение понятия «отказобезопасность ИС». Взаимосвязь функциональной надежности и функциональной безопасности ИС.
8. Трактовка понятия «киберзащищенность ИС». Угрозы и категории киберзащищенности для ИС.
9. Стадии информационной атаки и в чем они заключаются.
10. Типы компьютерных атак на ИС, поражающих ПО.
11. DoS-атаки.
12. Взаимосвязь функциональной и информационной безопасности критически важных систем. Процедуры оценки этой взаимосвязи.

13. Модель процессов возникновения уязвимостей и ошибок в ходе разработки ПО.

14. Группы проявления программных ошибок.

15. Ошибки оператора и серьезные негативные последствия таких ошибок. Приведите примеры.

16. Характерные недостатки эксплуатируемых программ. Приведите примеры.

17. Троянские программы. Приведите примеры.

18. Назначение основных вредоносных программ. Таксономия вредоносных программ.

19. Маршрутная карта функциональной надежности ПО.

20. Модели надежности ПО. Основные определения этих моделей.

21. Оценочная модель Джелинского — Моранды.

22. Оценочная модель Шика — Волвертона.

23. Оценочная модель Литтлвуда.

24. Оценочная модель Шумана.

25. Измерительные модели Коркорэна, Пальчуна, Нельсона. Оценка безопасности ПО на базе модели Нельсона.

26. Основные группы показателей функциональной надежности и функциональной безопасности ПО. Связь показателей и свойств надежности ПО.

27. Рекомендации по разработке спецификации требований к программам.

28. Защитное программирование.

29. Способы многоверсионного программирования.

30. Методы и способы создания проекта надежного ПО.

31. Способы обеспечения надежности системы при интеграции программных и аппаратных средств.

32. Осуществление процессов эксплуатации, сопровождения и конфигурации программных средств.

33. Требования к функциональной надежности и архитектуре ПО критически важных систем.

34. Средства и системы тестирования программного обеспечения при испытаниях его на технологическую безопасность.

35. Способы анализа программных средств на предмет наличия (отсутствия) недекларированных возможностей.

36. Основные этапы построения программно-аппаратных комплексов для контроля технологической безопасности программ.

37. Средства и комплексы защиты программ от компьютерных вирусов.

38. Типы обфускаторов программ и их характеристика.

39. Средства обеспечения целостности и достоверности используемого программного кода.

40. Средства защиты программ от несанкционированного копирования.

41. Достоинства и недостатки статистических и динамических способов исследования ПО. Принципы работы дизассемблеров, декомпиляторов, трассировщиков, следящих систем при исследовании ПО.

42. Способы проведения испытаний ПО, оценки качества и сертификации программных средств. Состав методического обеспечения проведения испытаний программ.

43. Показатели качества ПО разных уровней. Последовательность операций при выборе номенклатуры показателей качества ПО. Оценка значений показателей качества ПО.

44. Основные этапы испытания ПО. Последовательность действий при этих испытаниях.

45. Технология создания сложных программных комплексов. Действия разработчиков при обеспечении технологической безопасности ПО.

46. Структурно-функциональная схема инструментальных средств поддержки создания безопасного программного обеспечения.

47. Этапы контроля безопасности общего и специального ПО на этапе исследования и испытаний ПО.

48. Требования к контрольно-испытательному стенду испытания технологической безопасности ПО и принципы его построения. Достоинства и недостатки существующих операционных сред для такого стенда.

49. Существующие на отечественном рынке антивирусные комплексы, их основные достоинства и недостатки. Базовый функционал антивирусных программ.

50. Существующие на отечественном рынке средства обеспечения целостности и достоверности используемого программного кода и средств защиты программ от несанкционированного копирования, их основные достоинства и недостатки.

51. Отечественные нормативные акты, регламентирующие деятельность в области обеспечения надежности и безопасности программного обеспечения.

52. Виды подтверждения соответствия информационных систем и их характеристика.

53. Порядок обработки результатов испытаний и принятия решения о подтверждении соответствия информационных систем требованиям стандартов.

54. Виды испытаний, необходимые для подтверждения соответствия требованиям качества и безопасности ПО и их назначение.

55. Процедура декларирования соответствия ПО по требованиям стандартов качества и функциональной безопасности.

56. Процедура сертификационных испытаний ПО на отсутствие недекларированных возможностей.

4 Методические указания для обучающихся по освоению дисциплины

Приступая к изучению дисциплины «Безопасность программного обеспечения», студент должен ознакомиться с содержанием данной «Рабочей учебной программы дисциплины» с тем, чтобы иметь четкое представление о своей работе. Изучение дисциплины осуществляется на основе выданных студенту преподавателем рекомендаций по выполнению всех заданий, предусмотренных учебным планом и программой.

В первую очередь необходимо уяснить цель и задачи изучаемой дисциплины, оценить объем материала, познакомиться с предложенной и подобрать основную и дополнительную литературу, выявить наиболее важные проблемы, стоящие по вопросам изучаемой дисциплины.

Выполнение заданий осуществляется в соответствии с учебным планом и программой. Они должны выполняться в соответствии с методическими рекомендациями, выданными преподавателем, и представлены в установленные преподавателем сроки.

Работая с учебниками и учебными пособиями, целесообразно законспектировать тот материал, который не сообщался студентам на лекциях.

На занятиях лекционного и практического характера студентам для работы требуется: тетрадь для записи лекций и заданий.

Для успешного овладения программой дисциплины необходимо выполнять следующие требования:

— посещать все лекционные и практические занятия;

— все рассматриваемые на лекциях и практических занятиях темы и вопросы обязательно фиксировать в тетради;

— в случае пропуска занятий по каким-либо причинам необходимо обязательно самостоятельно изучать соответствующий материал в Moodle, фиксируя записи в тетради, а также выполнять практические задания.

Подготовка к зачету с оценкой осуществляется по представленным в списке основной и дополнительной литературе, а также частично по нормативным документам. В учебниках и учебных пособиях содержатся одноименные параграфы, что позволит успешно

подготовиться к зачету с оценкой. Рекомендуемые литература и интернет-ресурсы будут полезны при выполнении практических заданий, при чтении кода программ и для подготовки к тестированиям. В рекомендуемых интернет-ресурсах также можно найти ссылки на научные журналы по информационным технологиям и на форумы профессиональных сообществ программистов.

Методические рекомендации по составлению конспекта

Конспект — сложный способ изложения содержания книги или статьи в логической последовательности. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта. Выделите главное, составьте план, представляющий собой перечень заголовков, подзаголовков, вопросов, последовательно раскрываемых затем в конспекте.

Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

При оформлении конспекта необходимо стремиться к емкости каждого предложения.

Методические рекомендации по составлению опорного конспекта

Опорный конспект — вид внеаудиторной самостоятельной работы студента по созданию краткой информационной структуры, обобщающей и отражающей суть материала лекции, темы учебника.

Опорный конспект — это наилучшая форма подготовки к ответу на вопросы.

Основная цель опорного конспекта — облегчить запоминание. Этапы составления опорного конспекта:

1. Изучить материалы темы, выбрать главное и второстепенное;

2. Установить логическую связь между элементами темы;

3. Представить характеристику элементов в краткой форме;

4. Выбрать опорные сигналы для акцентирования главной информации и отобразить в структуре работы.

Методические рекомендации по прохождению тестирования

Тестирование — это исследовательский метод, который позволяет выявить уровень знаний, умений и навыков, способностей, а также их соответствие определенным нормам усвоения, путем выполнения испытуемым ряда специальных заданий.

Следует понимать, что тестовые задания могут быть представлены в различных формах:

— задания закрытой формы, в которых обучающийся выбирает один или несколько правильных ответов из заданного набора:

— задания на дополнение (открытые задания) требующие самостоятельного получения ответов:

— задания на установления соответствия (с множественным выбором), выполнение которых связано с выявлением соответствия между элементами нескольких множеств:

— задания на установление правильной последовательности, в которых от учащегося требует указать порядок действий или процессов и другие. Этапы подготовки к тестированию:

1. Внимательно прочитайте материал по конспекту, составленному на учебном занятии. Прочитайте тот же материал по учебнику, учебному пособию.

2. Постарайтесь разобраться с непонятным, в частности новыми терминами и конструкциями.

3. Ответьте на контрольные вопросы для самопроверки, имеющиеся в учебнике, конспекте и т. д.

4. Кратко перескажите содержание изученного материала «своими словами».

5. Выучите определения основных понятий, условные обозначения, формулы и конструкции.

Подготовка к практическим занятиям

В ходе подготовки к практическим занятиям необходимо изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях, ознакомиться с программным обеспечением. Следует дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой.

Заканчивать подготовку следует закреплением материала с использованием соответствующих программных продуктов.

Все практические задания, предусмотренные рабочей программой, представлены в фонде оценочных средств по дисциплине.

Критерии оценивания выполненных практических работ:

— правильность выполнения работы (отсутствие фактических, логических и других ошибок);

— полнота выполнения работы;

— своевременность выполнения;

— правильность оформления отчета.

За задания, выполненные позже установленного срока или с нарушениями требований к оформлению, оценка на балл снижается.

Порядок организации самостоятельной работы студентов

Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Целью самостоятельной работы студентов является: овладение практическими знаниями, профессиональными умениями и навыками деятельности по специальности, опытом творческой, исследовательской деятельности.

Самостоятельная работа студентов предполагает:

— самостоятельный поиск ответов и необходимой информации в рамках изучаемых тем;

— выполнение заданий для самостоятельной работы, в том числе тестов;

— изучение теоретического и лекционного материала, а также основной и дополнительной литературы при подготовке к практическим занятиям.

Самостоятельная работа студентов является обязательным элементом подготовки специалиста среднего звена.

5 Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»

Основная литература

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва: Издательство Юрайт, 2025. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/580668 (дата обращения: 16.08.2025).

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2025. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567283 (дата обращения: 16.08.2025).

3. Прохорова, О. В. Информационная безопасность и защита информации: учебник для СПО / О. В. Прохорова. — 6-е изд., стер. — Санкт-Петербург: Лань, 2025. — 124 с. — ISBN 978-5-507-52269-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/445250 (дата обращения: 16.08.2025). — Режим доступа: для авториз. пользователей.

4. Щербак, А. В. Информационная безопасность: учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567521 (дата обращения: 16.08.2025).

Дополнительная литература

1. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва: РИОР: ИНФРА-М, 2025. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2178344 (дата обращения: 16.08.2025). – Режим доступа: по подписке.

2. Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности: учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. — Москва: РИОР: ИНФРА-М, 2024. — 236 с. - ISBN 978-5-369-01788-3. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2140687 (дата обращения: 16.08.2025). – Режим доступа: по подписке.

3. Васильева, И. Н. Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. — Москва: Издательство Юрайт, 2025. — 310 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560977 (дата обращения: 16.08.2025).

4. Гагарина, Л. Г. Технология разработки программного обеспечения: учебное пособие / Л.Г. Гагарина, Е.В. Кокорева, Б.Д. Сидорова-Виснадул; под ред. Л.Г. Гагариной. — Москва: ФОРУМ: ИНФРА-М, 2025. — 400 с. — (Среднее профессиональное образование). — ISBN 978-5-8199-0812-9. — Текст: электронный. — URL: https://znanium.ru/catalog/product/2183867 (дата обращения: 16.08.2025). – Режим доступа: по подписке.

5. Запечников, С. В. Криптографические методы защиты информации: учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва: Издательство Юрайт,

2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536453 (дата обращения: 16.08.2025).

6. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления: монография / И.С. Клименко. — Москва: ИНФРА-М, 2024. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2052391 (дата обращения: 16.08.2025). – Режим доступа: по подписке.

7. Красов, А. В. Разработка защищенного программного обеспечения: учебное пособие / А. В. Красов, А. Ю. Цветков. — Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2023. — 154 с. — ISBN 978-5-89160-308-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/425906 (дата обращения: 16.08.2025). — Режим доступа: для авториз. пользователей.

8. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва: Издательство Юрайт, 2025. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560426 (дата обращения: 16.08.2025).

9. Новосадова, М. В. Справочник IT-терминов: справочник / М. В. Новосадова. — Москва; Вологда: Инфра-Инженерия, 2023. — 68 с. — ISBN 978-5-9729-1156-1. — Текст: электронный. — URL: https://znanium.com/catalog/product/2099119 (дата обращения: 16.08.2025). — Режим доступа: по подписке.

10. Окороков, В. А. Безопасность операционных систем / В. А. Окороков. — Санкт-Петербург: Лань, 2024. — 228 с. — ISBN 978-5-507-48297-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/367472 (дата обращения: 16.08.2025). — Режим доступа: для авториз. пользователей.

11. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для вузов / В. М. Фомичёв, Д. А. Мельников; под редакцией В. М. Фомичёва. — Москва: Издательство Юрайт, 2025. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560804 (дата обращения: 16.08.2025).

12. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты: учебник для вузов / В. М. Фомичёв, Д. А. Мельников; под редакцией В. М. Фомичёва. — Москва: Издательство Юрайт, 2025. — 245 с. — (Высшее

образование). — ISBN 978-5-9916-7090-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561432 (дата обращения: 16.08.2025).

13. Шитов, В. Н. Устройство и функционирование информационной системы: учебник / В. Н. Шитов. — Москва: КноРус. 2024. — 333 с. — ISBN 978-5-406-12882-4. — URL: https://book.ru/book/953436 (дата обращения: 16.08.2025). — Текст: электронный.

14. Штеренберг, С. И. Вредоносное программное обеспечение: учебное пособие / С. И. Штеренберг. — Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2024. — 71 с. — ISBN 978-5-89160-319-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/426137 (дата обращения: 16.08.2025). — Режим доступа: для авториз. пользователей.

Нормативные документы

1. PEP 8. Правила написания кода на Python. — URL: https://peps.python.org/pep-0008/

2. ГОСТ 12207 ИТ. Процессы жизненного цикла программных средств. — URL: https://normativ.kontur.ru/document?moduleId=9&documentId=212198&ysclid=mhqyd44gx109597256

3. ГОСТ 19.101-2024. Единая система программной документации. Виды программ и программных документов. (введен в действие 30.01.2025). — URL: https://protect.gost.ru/document.aspx?control=7&id=263735&ysclid=mhqygb9erh989749121

4. ГОСТ 19.101-77. Единая система программной документации (ЕСПД). — URL: https://rosgosts.ru/file/gost/35/080/gost_19.101-77.pdf

5. ГОСТ 19.201-78 Техническое задание, требования к содержанию и оформлению. — URL: https://rosgosts.ru/file/gost/35/080/gost_19.201-78.pdf

6. ГОСТ 19.401-78. Единая система программной документации. Текст программы. Требования к содержанию и оформлению. — URL: https://docs.cntd.ru/document/1200007651?ysclid=mhqzq4l03u398598150

7. ГОСТ Р ИСО/МЭК 15910-2002 Информационная технология (ИТ). Процесс создания документации пользователя программного средства. — URL: https://docs.cntd.ru/document/1200030141?ysclid=mhqzifmkdo827279089

8. Стандарты ISO C++. — URL: https://isocpp.org/std/the-standard

Интернет-ресурсы

1. Code Beautify (Code Formatter, JSON Beautifier, XML Viewer, Hex Converters и др.). — URL: https://codebeautify.org/

2. Dev.to. — URL: https://dev.to/?ysclid=mhqyzbvhla276227563

3. GitFlic. Российская платформа для работы с кодом. — URL: https://gitflic.ru/

4. Online Python IDE. — URL: https://www.online-python.com/

5. Stack Overflow (на русском). — URL: https://ru.stackoverflow.com/?ysclid=mhqyx9542h717626304

6. The Linux Kernel documentation. — URL: https://www.kernel.org/doc/html/latest/

7. SWEBOK: Руководство по основам программной инженерии. — URL: https://www.computer.org/education/bodies-of-knowledge/software-engineering

8. Документация по разработке приложений для Astra Linux. — URL: https://docs.astralinux.ru/latest/?ysclid=mhqz4o3x8q692967251

9. Документация по разработке приложений для Windows. — URL: https://learn.microsoft.com/ru-ru/windows/apps/

10. Компилятор C++ (онлайн) «Online CPP». — URL: https://www.online-cpp.com/

11. Компилятор C++ (онлайн) «Programiz». — URL: https://programiz.pro/ide/cpp

12. Научный журнал «ИТ-СТАНДАРТ» (ООО «Информационно-аналитический вычислительный центр»). — URL: https://www.elibrary.ru/title_about_new.asp?id=54046

13. Научный журнал «Моделирование и анализ информационных систем» (Ярославский государственный университет им. П.Г. Демидова). — URL: https://www.elibrary.ru/title_about_new.asp?id=25794

14. Научный журнал «Прикладная информатика» (Московский финансово-промышленный университет «Синергия»). — URL: https://www.elibrary.ru/title_about_new.asp?id=25599

15. Научный журнал «Программная инженерия» (ООО «Издательство «Новые технологии»). — URL: https://www.elibrary.ru/title_about_new.asp?id=32250

16. Реестр российского программного обеспечения. — URL: https://reestr.digital.gov.ru/

17. Роспатент. Федеральная служба по интеллектуальной собственности. — URL: https://rospatent.gov.ru/ru

18. РОССТАНДАРТ. Федеральное агентство по техническому регулированию и метрологии. — URL: https://www.rst.gov.ru/portal/gost

6 Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Для реализации дисциплины необходимы:

Лаборатория программирования и баз данных, включающая:

— компьютерный класс (15-20 рабочих мест) с современными ПК, объединенными в локальную сеть с выходом в Интернет;

— проектор и экран;

— маркерная или меловая доска;

— информационно-коммуникационные технологии;

— программное обеспечение.

Информационно-коммуникационные технологии

Локальная вычислительная сеть с организованным доступом к электронным образовательным ресурсам.

Система видеоконференцсвязи (Mts Link) для проведения дистанционных консультаций.

Виртуальная образовательная среда на базе LMS (Moodle) для размещения учебных материалов и проведения тестирования.

Система облачного хранения (Яндекс Диск) и системы для коллективной работы над проектами (Яндекс Документы, Mts Link.Доски).

Программное обеспечение

Windows 10/11, Linux (дистрибутивы Debian, Ubuntu, Astra или Alt), MS Visual Studio, MS Visual Studio Code, SQLite, PostgresSQL, pgAdmin, DBeaver, Python IDE, 1С:Предприятие, Eclipse IDE, Apache NetBeans, Spacemacs, AndroidStudio, Draw.io, StarUML 5, Inkscape, LibreOffice, Oracle VM VirtualBox, Notepad++.

Электронно-библиотечные системы (ЭБС)

1. ЭБС «BOOK.RU». — URL: https://book.ru/
2. ЭБС «Znanium». — URL: https://znanium.ru/
3. ЭБС «Айбукс». — URL: https://ibooks.ru/
4. ЭБС «Лань». — URL: https://e.lanbook.com/
5. ЭБС «Юрайт». — URL: https://urait.ru/
6. Электронные каталоги библиотеки СЗИУ РАНХиГС. — URL: https://sziu-lib.ranepa.ru/