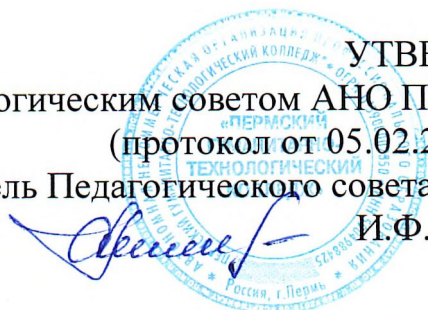


**Автономная некоммерческая организация профессионального образования  
«ПЕРМСКИЙ ГУМАНИТАРНО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»  
(АНО ПО «ПГТК»)**

**УТВЕРЖДЕНА**  
Педагогическим советом АНО ПО «ПГТК»  
(протокол от 05.02.2026 № 01)  
Председатель Педагогического совета, директор  
И.Ф. Никитина



**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ  
МЕЖДИСЦИПЛИНАРНОГО КУРСА**

**МДК 02.06 БЕЗОПАСНОСТЬ ПРОГРАММНОГО  
ОБЕСПЕЧЕНИЯ**

для специальности

**09.02.11 Разработка и управление программным обеспечением**  
(код и наименование специальности)

Квалификация выпускника  
**Программист**

Форма обучения  
**Очная**

Пермь 2026

Фонд оценочных средств междисциплинарного курса МДК 02.06 БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ составлен в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением (утвержден приказом Министерства Просвещения Российской Федерации от 24 февраля 2025 г. N 138).

Программа предназначена для студентов и преподавателей АНО ПО «ПГТК».

Автор – составитель: Могильникова Н.С., старший преподаватель.

Фонд оценочных средств междисциплинарного курса рассмотрена и одобрена на заседании кафедры математических и естественно-научных дисциплин, протокол, № 01 от 04.02.2026.

## **Содержание ФОС УД**

1. Паспорт фонда оценочных средств
  - 1.1. Область применения фонда оценочных средств
  - 1.2. Организация текущего контроля успеваемости и промежуточной аттестации по итогам освоения междисциплинарного курса
2. Контроль и оценка достижения запланированных результатов обучения
  - 2.1. Перечень вопросов и заданий для текущего контроля знаний
  - 2.2. Перечень вопросов и заданий для промежуточной аттестации
  - 2.3. Критерии оценивания ПА

## 1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

### 1.1 Область применения ФОС

Фонд оценочных средств (ФОС) представляет собой комплект материалов для проведения промежуточной аттестации и текущего контроля.

Результаты обучения - это усвоенные знания и освоенные умения по дисциплине в целях овладения предусмотренных стандартом общих и профессиональных компетенций, а также для оценки достижения обучающимися личностных результатов.

Фонд оценочных средств позволяет оценивать:

Код ОК, ПК	Уметь	Знать	Владеть навыками
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 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)	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 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	номенклатура информационных источников, применяемых в профессиональной деятельности приемы структурирования информации формат оформления результатов поиска информации современные средства и устройства	

	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	информатизации, порядок их применения программное обеспечение в профессиональной деятельности, в том числе цифровые средства психологические основы деятельности коллектива	
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 построения устных сообщений особенности социального и культурного контекста	
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)	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	

	<p>писать простые связные сообщения на знакомые или интересующие профессиональные темы</p>		
<p>ПК. 2.1 Проектировать модули программного обеспечения.</p>	<p>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 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</p>	<p>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 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</p>	<p>проектирования модулей ПО с учетом требований заказчика. создания архитектурных диаграмм и спецификаций модулей. определения интерфейсов и взаимодействия модулей в системе.</p>

<p>ПК. 2.2</p> <p>Разрабатывать модули программного обеспечения.</p>	<p>разрабатывать модули программного обеспечения с использованием различных языков программирования и технологий</p> <p>применять паттерны проектирования и структуры данных для создания эффективных и масштабируемых модулей</p> <p>анализировать требования и определять функциональность модуля</p> <p>создавать интерфейсы для взаимодействия с другими модулями и системами</p> <p>обеспечивать безопасность, производительность и масштабируемость при разработке модулей</p> <p>оптимизировать проектируемые модули для повышения их эффективности и качества</p> <p>работать с системой контроля версий</p> <p>улучшать производительность модулей, выявляя и устраняя узкие места</p> <p>проводить анализ и мониторинг производительности приложений</p> <p>применять инструменты для рефакторинга и оптимизации программного кода</p>	<p>язык программирования, основные конструкции, синтаксис</p> <p>паттерны проектирования</p> <p>структуры данных</p> <p>принципы создания интерфейсов для взаимодействия с другими модулями и системами, таких как REST API, SOAP</p> <p>работа с инструментальным программным обеспечением</p> <p>методы оптимизации кода и алгоритмов</p> <p>эффективные алгоритмы и структуры данных для повышения производительности</p> <p>многопоточность в программных модулях</p> <p>методы оптимизации сетевых протоколов для ускорения обмена данными</p> <p>кэширование данных</p> <p>управление памятью</p> <p>техники повышения производительности</p> <p>программного обеспечения</p>	<p>создание модулей программного обеспечения на различных языках программирования</p> <p>отладки и тестирования</p> <p>разработанных модулей</p> <p>применение структурного и объектно-ориентированного программирования</p> <p>оптимизации кода и алгоритмов</p> <p>программных модулей для увеличения производительности</p> <p>мониторинга и анализа</p> <p>производительности приложений</p>
<p>ПК. 2.3</p> <p>Выполнять интеграцию модулей и компонентов программного обеспечения.</p>	<p>интегрировать модули и компоненты, обеспечивая их взаимодействие</p> <p>работать с API и устанавливать соединения между компонентами</p>	<p>общих принципов функционирования аппаратных, программных и программно-аппаратных средств</p> <p>администрируемой информационно-коммуникационной системы</p>	<p>интеграции программных модулей и компонентов в единое программное решение</p> <p>работы с API и веб-сервисами для взаимодействия между модулями</p>

	отслеживать и устранять конфликты и ошибки интеграции анализировать и определять зависимости между модулями и компонентами работать с различными форматами данных и протоколами передачи данных	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	работы с интеграционными платформами и инструментами обеспечения совместимости и стабильности системы
ПК. 2.4 Выполнять тестирование и отладку программного обеспечения.	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 использовать системы контроля дефектов ПО составлять отчет о выполнении тестирования ПО	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 техники ручного тестирования техники автоматизированного тестирования жизненный цикл дефекта ПО принципы работы в системе контроля дефектов основные понятия о качестве ПО	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 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
ПК. 2.5 Осуществлять документирование программных модулей программного обеспечения.	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	создания технической документации для модулей документирования кода, API и интерфейсов работы со специализированным ПО по документированию программного кода

**1.2. Организация текущего контроля успеваемости и промежуточной аттестации по итогам освоения программы междисциплинарного курса**

В период обучения по образовательной программе СПО осуществляется текущий контроль успеваемости студентов, промежуточная аттестация по учебным дисциплинам и МДК.

Текущий контроль осуществляется в пределах учебного времени, отведенного на учебную дисциплину, оценивается по пятибалльной шкале. Текущий контроль проводится с целью объективной оценки качества освоения программы дисциплины, а также стимулирования учебной деятельности студентов, подготовки к промежуточной аттестации и обеспечения максимальной эффективности учебного процесса. Для оценки качества подготовки используются различные формы и методы контроля. Текущий контроль дисциплины осуществляется в форме устного опроса; защиты практических заданий, реферата, творческих работ; выполнения контрольных и тестовых заданий; решения ситуационных задач и других форм контроля, предусмотренных программой дисциплины.

Промежуточная аттестация проводится в форме, предусмотренной планом учебного процесса: экзамена, дифференцированного зачета, зачета.

В период сложной санитарно-эпидемиологической обстановки или других ситуациях невозможности очного обучения и проведения аттестации студентов колледж реализует образовательные программы или их части с применением электронного обучения, дистанционных образовательных технологий в предусмотренных законодательством формах обучения или при их сочетании, при проведении учебных занятий, практик, текущего контроля успеваемости, промежуточной аттестации обучающихся.

Форма промежуточной аттестации по дисциплине МДК 02.06 Безопасность программного обеспечения – дифференцированный зачет.

## **2. КОНТРОЛЬ И ОЦЕНКА ОСВОЕНИЯ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА**

### **2.1. Перечень вопросов и заданий для текущего контроля**

В результате текущей аттестации по МДК 02.06 Безопасность программного обеспечения осуществляется проверка сформированности умений и знаний, направленных на формирование соответствующих ФГОС СПО общих и профессиональных компетенций.

Перечень практических работ.

1. Ограничение доступа на вход в систему.
2. Идентификация и аутентификация пользователей.
3. Разграничение доступа.
4. Регистрация событий (аудит).
5. Контроль целостности данных
6. Уничтожение остаточной информации.
7. Распределение каналов в соответствии с источниками воздействия на информацию.
8. Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО.
9. Защита информации от несанкционированного копирования с использованием специализированных программных средств.
10. Применение средства восстановления остаточной информации на примере Foremost или аналога.
11. Применение специализированного программного средства для восстановления удаленных файлов.
12. Применение программ для безвозвратного удаления данных.

**Контрольные работы** организуются в компьютерных аудиториях и выполняются по заданию преподавателя с использованием изучаемого программного обеспечения.

1. Разграничение прав пользователей.

Определения понятий (изучить, включить в отчет):

- аутентификация,
- авторизация,
- администратор безопасности,
- симметричное и асимметричное шифрование,
- хеширование,
- политика безопасности.

Подготовить для включения в отчет о работе ответы на следующие вопросы:

- какие существуют способы аутентификации пользователей?
- в чем слабость парольной аутентификации?
- как может быть повышена надежность аутентификации с помощью паролей?
- какой может быть реакция системы на попытку подбора паролей?
- кому может быть разрешен доступ по чтению и по записи к базе учетных записей пользователей?

- как должны храниться пароли в базе учетных записей пользователей?
- в чем смысл объединения пользователей в группы?

2. Реализация политики безопасности в защищенных версиях операционной системы Windows.

Определение понятий (изучить, включить в отчет):

- аудит;
- событие безопасности;
- журнал (файл) аудита;
- политика аудита;
- интерактивный вход;
- сетевой доступ;

- домен компьютерной сети;
- цифровая подпись.

Подготовить для включения в отчет о работе ответы на следующие вопросы:

- какие события безопасности должны фиксироваться в журнале аудита?
- какие параметры определяют политику аудита?
- целесообразно ли с точки зрения безопасности компьютерной системы объединение в одном лице функций администратора и аудитора?
- целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?
- как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя (или другая аутентифицирующая информация)?
- нужно ли ограничивать права пользователей по запуску прикладных программ и почему?

3. Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows.

Подготовить для включения в отчет о работе определения понятий:

- дискреционная политика безопасности;
- мандатная политика безопасности;
- субъект доступа;
- объект доступа;
- виды доступа;
- монитор обращений;
- монитор безопасности объектов;
- домен безопасности;
- реестр операционной системы;
- контроль целостности объектов;
- ключ симметричного шифрования;
- ключи асимметричного шифрования.

Подготовить для включения в отчет о работе ответы на следующие вопросы:

- в чем достоинства и недостатки дискреционной политики безопасности?
- в чем достоинства и недостатки мандатной политики безопасности?
- в чем заключается тождественность объектов и тождественность субъектов компьютерной системы?
- кто определяет права доступа к папкам, файлам, принтерам при использовании дискреционной политики безопасности?
- каковы возможные пути нарушения политики безопасности в компьютерной системе?

- какие факторы влияют на определение размеров доменов безопасности?
- какая информация хранится в реестре Windows?

4. Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows XP/7.

Подготовить для включения в отчет о работе определения понятий:

- матрица доступа;
- дискреционный список контроля доступа;
- домен безопасности;
- журнал (файл) аудита;
- запись журнала аудита;
- стандарт безопасности.

Подготовить для включения в отчет о работе ответы на следующие вопросы:

- что такое Trusted Computer System Evaluation Criteria (TCSEC)?
- какие основные категории требований к защищенности компьютерных систем предложены в TCSEC, в чем их смысл?

- какие требования к компьютерным системам предъявляются по классу защиты C2 TCSEC?

- кто управляет дискреционным списком контроля доступа к объектам в операционной системе Windows XP?

- как должны использоваться записи журнала аудита событий безопасности?

- какие права доступа к файлу аудита имеет по умолчанию администратор системы?

- что такое консольное приложение Windows?

5. Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows XP

Цель работы: освоение системных программ Windows XP, программ из комплекта Windows NT Resource Kit и других программных средств, предназначенных для:

- просмотра и управления разрешениями на доступ к конфиденциальным объектам компьютерной системы;

- просмотра и анализа записей аудита;

- анализа соответствия реализуемой в компьютерной системе политики безопасности требованиям стандартов безопасности;

- дополнительной защиты базы учетных записей пользователей компьютерной системы и используемых ими рабочих станций.

Подготовить для включения в отчет о работе ответы на следующие вопросы:

- что такое Trusted Computer System Evaluation Criteria (TCSEC)?

- какие основные категории требований к защищенности компьютерных систем предложены в TCSEC, в чем их смысл?

- какие требования к компьютерным системам предъявляются по классу защиты C2 TCSEC?

- кто управляет дискреционным списком контроля доступа к объектам в операционной системе Windows XP?

- как должны использоваться записи журнала аудита событий безопасности?

- какие права доступа к файлу аудита имеет по умолчанию администратор системы?

- что такое консольное приложение Windows?

Наивысшая оценка отчета о работе предусматривается в диапазоне от 2 до 5 баллов, в зависимости от сложности задания.

При оценке работы студента учитываются:

• уверенность действий при работе с изучаемым программным обеспечением;

• правильность выполнения необходимых шагов в лабораторной работе и адекватность / корректность полученного результата;

• умение самостоятельно находить способы решения возникающих проблем с помощью изучаемого программного обеспечения;

• способность ответить на вопросы преподавателя о последовательности выполненных шагов для получения результата.

### **ТЕМЫ ДОКЛАДОВ С ПРЕЗЕНТАЦИЯМИ**

Подготовка презентации на 12-15 слайдов с устным докладом по заданной тематике:

Примерный перечень тем:

1. ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» Части 1, 2, 3

2. Анализ методов повышения надежности хранения информации на жестких магнитных дисках

3. Анализ средств защиты от спама

4. Анализ методов обеспечения безопасности домашней сети

5. Анализ методов изучения поведения нарушителей безопасности компьютерных систем

6. Анализ методов перехвата паролей пользователей компьютерных систем и

методов противодействия им

7. Сравнительный анализ антивирусных пакетов
8. Анализ методов обеспечения безопасности электронного магазина
9. Анализ методов организации антивирусной защиты компьютерных систем
10. Сравнительный анализ систем обнаружения атак
11. Анализ средств безопасности в пакете Microsoft Office
12. ГОСТ Р ИСО/МЭК ТО 15446 «Информационная технология. Методы и

средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности»

13. Сравнительный анализ средств защиты электронной почты

14. ГОСТ Р ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».

Критерии оценки доклада с презентацией:

**13-15 баллов** выставляется студенту, если:

- проведенное исследование и изложенный в докладе материал соответствует заданной теме;
- представленные в докладе сведения отвечают требованиям актуальности и новизны;
- продумана структура и стиль сопроводительной презентации;
- студент способен ответить на вопросы преподавателя по теме доклада.

**6-12 баллов:**

- представленный в докладе материал соответствует заданной теме, однако присутствуют недостатки в связности изложения и структуре сопроводительной презентации;
- не все выводы носят аргументированный и доказательный характер.

**1-5 баллов:**

- студент способен изложить материал доклада, однако наблюдаются отклонения от заданной темы;
- сопроводительная презентация подготовлена, но плохо соотносится с представленным докладом.

**0 баллов:**

- материал не соответствует заданной теме;
- отсутствует сопроводительная презентация к докладу;
- студент не освоил материал полностью и не способен ответить на вопросы преподавателя по теме доклада

**Критерии оценивания выполнения практического задания**

- рациональное распределение времени по этапам выполнения задания
- обращение в ходе задания к информационным источникам
- знание терминологии
- скорость выполнения
- количество предложенных вариантов решения поставленной задачи.

Вопросы для устного опроса:

1. Концепция информационной безопасности.
2. Каналы утечки информации.
3. Виды ПО. Назначение и функции ОС.
4. Классификация операционных систем.
5. Локальные и удаленные атаки и методы взлома ОС.
6. Защита от локального НСД.
7. Протокол Kerberos.
8. Протокол S/key
9. Идентификация и аутентификация.
10. Подсистема аутентификации Windows.

11. Разграничение доступа.
12. Избирательный и мандатный метод разграничения доступа.
13. Аудит.
14. Политика аудита.
15. Фрагментарный и комплексный подход к построению ОС.
16. Методы анализа сетевой информации.
17. Защищенность БД
18. Модели безопасности БД

Тестовое задание	Вариант ответа
<b>1. Защита информации это-</b>	<p>А) потенциальная возможность неправомерного преднамеренного или случайного воздействия , приводящее к потере или разглашению информации. Б) реализация права на государственную тайну и конфиденциальную информацию</p> <p><b>В) устранение или нейтрализация негативных источников, причин и условий воздействия на информацию</b></p> <p><b>Г) правовые, организационные и технические меры, направленные на обеспечение защиты информации</b></p>
<b>2. Каналы утечки информации - это</b>	<p>А) это комплексы специального технического и программного обеспечения, предназначенные для предотвращения утечки информации</p> <p><b>Б) методы и пути утечки информации из информационной системы</b></p> <p>В) потенциальная возможность неправомерного преднамеренного или случайного воздействия</p> <p>Г) соблюдение конфиденциальности информации ограниченного доступа</p>
<b>3. Существуют следующие виды ПО (добавьте недостающее).</b>	<p>А) Прикладное ПО</p> <p>Б) Системное ПО</p> <p><b>В) Инструментальное ПО</b></p>

4. К функциям ОС относится :	<p>А) поддержка работы всех программ, обеспечение их взаимодействия с аппаратурой</p> <p><b>Б) управление процессором путем чередования выполнения программ;</b></p> <p>В) обработка прерываний и синхронизация доступа к ресурсам вычислительной системы;</p> <p><b>Г) управление памятью путем выделения программам на время их выполнения требуемой памяти;</b></p>
5. Операционная система Windows является:	<p>А) многозадачной</p> <p>Б) однозадачной</p> <p><b>В) многопользовательской</b></p> <p>Г) однопользовательской</p>
6. Атаки на ОС бывают:	<p>А) Локальными</p> <p>Б) Глобальными</p> <p><b>В) Удаленными</b></p> <p>Г) Близкими</p>
7. Профессиональный взлом имеет следующую структуру (восстановите последовательность)	<p>А) попытка внедрения вредоносных программ</p> <p>Б) поиск уязвимостей в ПО ЗИ</p> <p>В) тщательный анализ ПО</p> <p>Г) анализ выбранной политики безопасности</p> <p><b>Ответ Г,В,Б,А</b></p>
8. Когда пользователь знает что-то, что подтверждает его подлинность, то существуют следующие способы аутентификации:	<p>А) <b>парольная аутентификация</b></p> <p>Б) аутентификация по магнитному носителю</p> <p>В) модель рукопожатия</p> <p>Г) аутентификация по характеристикам работы пользователя</p>
9. Когда пользователь что-то имеет, что подтверждает его подлинность, то существуют следующие способы аутентификации:	<p>А) парольная аутентификация</p> <p><b>Б) аутентификация по магнитному носителю</b></p> <p>В) модель рукопожатия</p> <p>Г) аутентификация по характеристикам работы пользователя</p>
10. К защите от удаленного НСД можно отнести:	<p>А) модель рукопожатия</p> <p><b>Б) Протокол Kerberos</b></p> <p>В) Аутентификация по биометрическим характеристикам</p> <p>Г) Аутентификация по росписи мышью</p>



<b>11. Целью защиты информации является:</b>	<p>А) предотвращение хищения, утечки, искажения, утраты и подделки информации;</p> <p><b>Б) предотвращение несанкционированных действий по уничтожению, модификации, копированию и блокированию информации;</b></p> <p>В) реализация права на государственную тайну и конфиденциальную информацию</p> <p>Г) выявление правил и норм поведения человека, направленные на обеспечение безопасности информации</p>
<b>12. К основным видам средств защиты информации относится:</b>	<p>А) <b>нормативно-правовые</b></p> <p>Б) <b>Технические</b></p> <p>В) Экологические</p> <p>Г) Этнические</p>
<b>13. Технические средства защиты - это</b>	<p>А) правила, меры и мероприятия, регламентирующие вопросы доступа, хранения, применения и передачи информации</p> <p><b>Б) это комплексы специального технического и программного обеспечения</b></p> <p>В) правила и нормы поведения, направленные на обеспечение безопасности информации</p> <p>Г) законы и другие правовые акты, а также механизмы их реализации, регламентирующие информационные отношения в обществе</p>
<b>14. К каналам утечки информации относится:</b>	<p>А) <b>Магнитный канал</b></p> <p><b>Б) Виброакустический канал</b></p> <p><b>В) Лазерный канал</b></p> <p>Г) Специальный канал</p>
<b>15. К назначению ОС относится:</b>	<p>А) управление процессором путем чередования выполнения программ;</p> <p>Б) обработка прерываний и синхронизация доступа к ресурсам вычислительной системы;</p> <p>В) управление памятью путем выделения программам на время их выполнения требуемой памяти;</p> <p><b>Г) поддержка работы всех программ, обеспечение их взаимодействия с аппаратурой;</b></p>
<b>16. Многопроцессорная обработка в ОС бывает:</b>	<p>А) <b>Симметричной</b></p> <p>Б) Квадратичной</p> <p>В) Полной</p> <p>Г) <b>Ассиметричной</b></p>

<b>17. К локальной защите от НСД относится:</b>	А) Аутентификация на основе биометрических характеристик Б) Протокол СПАР В) Парольная аутентификация Г) Протокол РАР
<b>18. Когда пользователь и есть то лицо, за которое себя выдает то существуют следующие способы аутентификации:</b>	А) парольная аутентификация Б) аутентификация по магнитному носителю В) модель рукопожатия Г) аутентификация по характеристикам работы пользователя
Тестовое задание	Вариант ответа
<b>19. Какой протокол направленный для защиты от удаленного НСД основан на использовании одноразовых паролей.</b>	А) РАР Б) СНАР В) S/KEY Г) Kerberos
<b>20. К недостаткам дискреционного управления доступом относится:</b>	А) нельзя контролировать утечку конфиденциальной информации Б) неудобство для пользователя В) нет опасности утечки конфиденциальной информации Г) слабая защита от вредоносных программ

#### Критерии оценки;

Количество правильных ответов	Процент выполнения	Оценка
19-20	более 90%	Отлично
17-18	80-90%	Хорошо
14-16	60-79%	Удовлетворительно
До 13	менее 60%	Неудовлетворительно

## 2.2. Перечень вопросов и заданий для промежуточной аттестации

Дифференцированный зачет

Контрольные вопросы:

1. Базовые свойства информации применительно к ИБ.
2. Идентификация, аутентификация, авторизация.
3. Анализ угроз ИБ.
4. Признаки классификации угроз.
5. НСД к информации. Способы получения НСД.
6. Общие критерии безопасности.
7. Концепции общих критериев.
8. Политика безопасности организации.
9. Распределение ролей и обязанностей администраторов и пользователей сети.
10. Структура политики безопасности.
11. Уровни политики безопасности.
12. Процедуры безопасности.
13. Основные понятия криптографической защиты информации.
14. Симметричные криптосистемы шифрования.
15. Ассиметричные криптосистемы шифрования.
16. Электронная цифровая подпись и функция хэширования.
17. Аутентификация, авторизация и администрирование действий пользователей.
18. Аутентификация на основе паролей.
19. Угрозы безопасности ОС.
20. Понятие защищенной ОС.
21. Основные функции подсистемы защиты ОС.
22. Разграничение доступа к объектам ОС.
23. Аудит.
24. Технология межсетевых экранов.
25. Функции МЭ.
26. Дополнительные возможности МЭ.
27. Проблемы безопасности МЭ.
28. Алгебраические структуры. Группы. Кольца. Поля. Кольца многочленов
29. Алгебраические структуры. Поля  $GF(2^n)$ . Полиномы
30. Современные блочные шифры. Подстановка, транспозиция. Атаки на блочные шифры.
31. Полноразмерные ключевые шифры. Шифр без ключа
32. Компоненты современного блочного шифра. Р-блоки.
33. Компоненты современного блочного шифра. S-блоки
34. Компоненты современного блочного шифра. Понятие операции "исключающее или".
35. Компоненты современного блочного шифра. Операция циклического сдвига.
36. Компоненты современного блочного шифра. Замена. Разбиение и объединение
37. Составной шифр. Рассеивание и перемешивание. Понятие раунда
38. Схема Фейстеля и не-Фейстеля
39. Современные блочные криптосистемы
40. Симметричные стандарты шифрования – DES
41. Симметричные стандарты шифрования – AES
42. Симметричные стандарты шифрования - ГОСТ 28147-89
43. Современные поточные шифры
44. Синхронные шифры потока. Одноразовый блокнот
45. Матрица состояний потоковых шифров. Алгоритм шифрования RC4
46. Линейные генераторы псевдослучайных последовательностей.

47. Генераторы псевдослучайных последовательностей. Датчики Фибоначчи
48. Генераторы псевдослучайных последовательностей. Алгоритм BBS
49. Принципы использования ГПСЧ при потоковом шифровании
50. Понятие простого числа. Испытание простоты чисел
51. Функция Эйлера. Понятие хеш-функции
52. Шифры с открытыми ключами. Асимметричные системы шифрования ГОСТ 94
53. Шифры с открытыми ключами. Асимметричные системы шифрования RSA
54. Криптосистемы на основе эллиптических уравнений
55. Экономика информационной безопасности на примере оценки криптосистем
56. Оценка эффективности криптографической защиты
57. Квантовые алгоритмы шифрования

#### **Типовые практические задания к дифференцированному зачету:**

1. Кольца многочленов. Задача на построение кольца многочленов
  2. Конечные поля. Задача на построение конечных полей заданного порядка
  3. Задача на построение модели блочного шифра подстановки как шифра перестановки
  4. Задача на составление отношений между входами/выходами для S-блока
  5. Задача на реализацию компонентов современного блочного шифра. P-блоки.
  6. Задача на реализацию компонентов современного блочного шифра. Понятие операции "исключающее или".
  7. Задача на реализацию компонентов современного блочного шифра. Операция циклического сдвига.
  8. Задача на реализацию компонентов современного блочного шифра. Замена.
- Разбиение и объединение**
9. Задача на реализацию шифрования по схеме Фейстеля
  10. Задача на реализацию алгоритма шифрования - DES
  11. Задача на реализацию алгоритма шифрования - AES
  12. Задача на реализацию алгоритма шифрования - ГОСТ 28147-89
  13. Задача на реализацию алгоритма шифрования RC4
  14. Задача на реализацию алгоритма шифрования с помощью линейного конгруэнтного ГПСЧ
  15. Задача на реализацию алгоритма шифрования с помощью ГПСЧ с задержкой по методу Фибоначчи
  16. Задача на реализацию алгоритма шифрования с помощью алгоритма BBS
  17. Задача на реализацию алгоритма шифрования Эль Гамала
  18. Задача на реализацию алгоритма шифрования RSA
  19. Задача на применение протокола обмена ключами Диффи-Хелмана
  20. Задача на применение ЭЦП на основе алгоритма шифрования с открытым ключом

#### **Критерии оценивания ответа**

**Оценка «отлично»** выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий.

**Оценка «хорошо»** выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения.

**Оценка «удовлетворительно»** выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, Недостаточно формулировки, нарушения логической последовательности в изложении программного

материала.

**Оценка «неудовлетворительно»** выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.

**Критерии оценивания выполнения практического задания**

- рациональное распределение времени по этапам выполнения задания
- обращение в ходе задания к информационным источникам
- знание терминологии
- скорость выполнения
- количество предложенных вариантов решения поставленной задачи.