Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»

Факультет информационных технологий и анализа больших данных
Кафедра «Информационная безопасность»

ПРОГРАММА

вступительного испытания
для поступающих на обучение по программам подготовки научных и научно-педагогических кадров в аспирантуре
«МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ,
ИНФОРМАЦИОННАЯ БЕЩОПАСНОСТЬ»

Москва — 2026

Программа вступительного испытания на обучение по программе подготовки научных и научно-педагогических кадров в аспирантуре по направлению 10.06.01 «Информационная безопасность»

А.В. Иванов, С.И. Козьминых, А.С. Марков, Д.А. Мельников, А.В. Царегородцев, - М.: Финансовый университет при Правительстве Российской Федерации, 2024. – 29 с.

Рецензенты:

Программа «Методы и системы защиты информации, информационная безопасность» предназначена для подготовки к сдаче вступительного испытания в аспирантуру по направлению 10.06.01 «Информационная безопасность», научная специальность 2.3.6. «Методы и система защиты информации, информационная безопасность»

Учебное издание

Программа вступительного испытания
для поступающих на обучение по программе подготовки
научных и научно-педагогических кадров в аспирантуре
по направлению 10.06.01 «Информационная безопасность». образовательная программа «Методы и системы защиты информации,
информационная безопасность»

Компьютерный набор и верстка:

Формат 60×90/16. Гарнитура Times New Roman
Усл.п.л. – 1,8. Тираж 30 экз.

Отпечатано в Финансовом университете

Содержание

I. Общие положения

Предназначение программы. Программа вступительного испытания «Методы и системы защиты информации, информационная безопасность» предназначена для лиц, поступающих по программе подготовки научных и научно-педагогических кадров в аспирантуре по направлению 10.06.01 «Информационная безопасность», научная специальность 2.3.6. «Методы и система защиты информации, информационная безопасность»

Цель и задачи программы. определение степени готовности поступающего к освоению основной образовательной программы аспирантуры по программе подготовки научно-педагогических кадров в аспирантуре по направлению 10.06.01 «Информационная безопасность», научная специальность 2.3.6. «Методы и система защиты информации, информационная безопасность». В рамках общей цели выделяются следующие задачи: определить пределы повторения материала по дисциплинам учебных курсов бакалавриата и магистратуры, необходимые для успешного прохождения вступительных испытаний.

Поступающий в аспирантуру на обучение по программе подготовки научных и научно-педагогических кадров по направлению 10.06.01 «Информационная безопасность», научная специальность 2.3.6. «Методы и система защиты информации, информационная безопасность» должен иметь глубокие знания как теории, так и практики в области информационной безопасности. Кроме того, обязательным является знание нормативных и законодательных актов Российской Федерации, регулирующих методы и систему защиты информации.

Вступительный экзамен в аспирантуру по специальной дисциплине по научной специальности 2.3.6. «Методы и система защиты информации, информационная безопасность» проводится в комбинированной форме: компьютерное тестирование и защита исследовательского проекта.

Тесты и защита исследовательского проекта являются неотъемлемыми частями вступительного испытания. Неявка на любую часть считается неявкой на экзамен.

Компьютерное тестирование содержит различные формы тестовых заданий. Исследовательский проект пишется по конкретной научной дисциплине и размещается в личном кабинете поступающего. Защита исследовательского проекта проходит в очной форме.

II. Содержание программы вступительного испытания

Раздел II.I. Компьютерное тестирование

Тема 1. Основные понятия и принципы теории информационной безопасности

1. Понятие национальной безопасности; виды безопасности.

2. Информационная безопасность в системе национальной безопасности Российской Федерации.

3. Доктрина информационной безопасности Российской Федерации. Органы государственной власти, регулирующие деятельность в области обеспечения информационной безопасности.

4. Основные термины и определения в области информационной безопасности.

5. Информационная безопасность и защита информации. Понятие угрозы безопасности информации.

6. Основные аспекты информационной безопасности: конфиденциальность, целостность, доступность.

7. Модели оценки ущерба от реализации угроз информационной безопасности.

8. Классификация угроз информационной безопасности.

9. Виды информации, методы и средства обеспечения информационной безопасности.

10. Способы нарушения конфиденциальности, целостности и доступности информации.

11. Основы комплексного обеспечения информационной безопасности.

12. Методы, модели и стратегии обеспечения информационной безопасности.

13. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

14. Аттестация объектов информатизации по требованиям безопасности информации: аттестация автоматизированных систем, средств связи, обработки

и передачи информации; аттестация помещений; аттестация технических средств, установленных в выделенных помещениях.

15. Лицензирование и сертификация в области защиты информации.

16. Правовые основы защиты информации.

17. Организационные основы защиты информации.

18. Основные вехи истории возникновения и развития защиты информации как самостоятельной отрасли человеческой деятельности.

19. Этапы формирования современных научно-практических основ защиты информации.

20. Обеспечение информационной безопасности информационных систем.

21. Структура документов, разрабатываемых для документирования требований политики безопасности к информационным системам.

22. Событие и инцидент информационной безопасности. Управление инцидентами информационной безопасности.

Тема 2. Организация ЭВМ и вычислительных сетей

1. Классификация и краткая характеристика типов современной компьютерной техники. Архитектура и структура современной компьютерной техники.

2. Элементная база современной компьютерной техники. Микропроцессоры. Понятие микропроцессорной системы. Обобщѐнная структура микропроцессорной системы.

3. Системная магистраль. Организация и структура памяти, системы прерывания; системы ввода-вывода; периферийные устройства.

4. Классификация систем хранения данных: локальные дисковые накопители, RAID-массивы, сети хранения данных (SAN), ленточные библиотеки.

5. Модели управления хранением данных. Международные стандарты в области хранения данных.

6. Программное обеспечение современной компьютерной техники. Системное и прикладное программное обеспечение (ПО).

7. Основные семейства операционных систем: UNIX-подобные (AIX, Solaris, FreeBSD, Linux, Android, MAC OS X и пр.), Windows, OS X. Специализированные операционные системы. ПО с открытым исходным кодом и проприетарное ПО.

8. Типология системного ПО: СУБД, мониторы виртуальных машин, ПО среднего слоя (middleware) и др. Типология прикладного ПО: CRM, CMS, CAD и др.

9. Концепция виртуализации вычислительных средств. Понятие монитора виртуальных машин. Облачные среды. Сервисы, предоставляемые облачными провайдерами для пользователей. Интерфейсы прикладного программирования (API) облачных сервисов для разработчиков прикладного ПО

10. Понятие открытой информационной системы. Предпосылки возникновения концепции открытых систем. Классификация информационных систем по назначению и сфере применения.

11. Локальные и глобальные вычислительные сети, типовые конфигурации, маршрутизация.

12. Основные протоколы обмена данными в вычислительных сетях.

13. Системы управления базами данных, реляционная, иерархическая и сетевая модели, распределенные БД.

14. Деревья и графы, их представление в ЭВМ, обходы графов.

15. Алгоритмы на графах, выделение компонент связности.

16. Кратчайшие пути в графе, минимальный остов графа.

17. Задача сортировки и основные алгоритмы сортировки.

18. Поиск информации методом хеширования.

19. Контрольно-испытательные и логико- аналитические методы анализа безопасности программ.

20. Методы и средства хранения ключевой информации в ЭВМ.

21. Защита программ от изучения, защита от изменения, контроль целостности.

22. Защита от разрушающих программных воздействий.

Тема 3. Криптографическая защита информации

1. Классическая криптография. Шифры замены и шифры перестановки. Шифры полиалфавитной замены.

2. Определение поточного шифра. Требования к стойкости поточного шифра. Конструкции поточных шифров. Синхронные и самосинхронизирующиеся поточные шифры. Групповые шифры гаммирования, шифры модульного гаммирования. Шифр Вернама. Одноразовый блокнот.

3. Генераторы случайных и псевдослучайных чисел. Основные принципы построения. Равномерно распределенные случайные последовательности, псевдослучайные последовательности. Требования к управляющей гамме генератора псевдослучайных чисел: длина периода, линейная сложность и т.д.

4. Конструкции криптографических генераторов случайных и псевдослучайных двоичных последовательностей: фильтрующие и комбинирующие генераторы, схемы с внешним управлением, схемы с самоуправлением, генераторы с дополнительной памятью.

5. Критерии оценки качества криптографических генераторов. Постулаты Голомба, пакет статистических тестов NIST. Критерий хи-квадрат.

6. Симметричные блочные шифры. Принципы построения подстановки итеративного симметричного блочного шифра. Конструкции блочных шифров: шифры, основанные на схеме Фейстеля, SP-сети.

7. Режимы шифрования: простая замена, сцепление блоков шифртекста, гаммирование с обратной связью по шифртексту, гаммирование с внутренней обратной связью, режим счетчика.

8. Симметричные схемы аутентификации сообщений на основе блочных шифров.

9. Криптографические хэш-функции и их свойства. Криптографические хэш-функции в российских и международных стандартах.

10. Симметричные схемы аутентификации сообщений на основе криптографических хэш-функций.

11. Симметричные схемы аутентифицированного шифрования. Режимы аутентифицированного шифрования в российских и международных стандартах.

12. Вычислительно сложные задачи, используемые в асимметричной криптографии. Арифметические алгоритмы, используемые в асимметричной криптографии. Генерация параметров и ключей асимметричных криптосхем.

13. Открытое распределение ключей. Протокол Диффи-Хеллмана.

14. Определение схемы открытого шифрования. Стойкость схем открытого шифрования. Сравнительная оценка симметричных шифров и схем открытого шифрования.

15. Определение схемы электронной подписи. Стойкость схем электронной подписи. Сравнительная оценка симметричных и асимметричных методов аутентификации сообщений.

16. Шифры замены и перестановки, их свойства, композиции шифров.

17. Криптостойкость шифров, основные требования к шифрам.

18. Теоретическая стойкость шифров, совершенные и идеальные шифры.

19. Методы получения случайных последовательностей, их использование в криптографии.

20. Криптографические протоколы. Протоколы распределения ключей.

21. Парольные системы разграничения доступа.

22. Стойкость систем с открытыми ключами.

Тема 4. Методы математического моделирования

1. Методы решения систем линейных уравнений.
2. Методы интерполяции.
3. Методы численного интегрирования.
4. Методы численного решения дифференциальных уравнений.
5. Численные методы нахождения экстремумов функций.

6. Элементы комбинаторики: перестановки, выборки, сочетания и размещения без повторений.

7. Сочетания и размещения с повторениями, биномиальные коэффициенты, их свойства.

8. Алгебра логики, формулы алгебры логики, высказывания и операции, построение формул.

9. Случайные величины, математическое ожидание и дисперсия,

10. Основные законы распределения случайной величины.

11. Центральная предельная теорема.

12. Цепи Маркова.

13. Система массового обслуживания без очереди и с очередью.

Тема 5. Методы и средства технической защиты информации

1. Структура, классификация и основные характеристики технических каналов утечки информации.

2. Побочные электромагнитные излучения и наводки.

3. Классификация средств технической разведки, их возможности.

4. Концепция и методы инженерно-технической защиты информации.

5. Методы скрытия речевой информации в каналах связи.

6. Методы обнаружения и локализации закладных устройств.

7. Методы подавления опасных сигналов акустоэлектрических преобразователей.

8. Методы подавления информативных сигналов в цепях заземления и электропитания.

9. Виды контроля эффективности защиты информации.

10. Методы расчета и инструментального контроля показателей защиты информации.

11. Утечка информации от офисной аппаратуры.

12. Упрощенная методика определения дальности, на которой возможен перехват ПЭМИН.

13. Утечка информации от вспомогательной аппаратуры и кабелей, проходящих через помещение. Привести примеры.

14. Несанкционированный съем информации с помощью радиозакладок.

15. Технические характеристики радиозакладок.

16. Прослушивание информации от пассивных закладок.

17. Структурная схема полуактивного микрофона.

18. Приемники информации с радиозакладок.

19. Конспирационные признаки радиозакладок.

20. Методы пассивной защиты от утечки по электромагнитному каналу.

21. Технические средства, предназначенные для поиска работающих радиозакладок.

22. Поиск радиозакладок нелинейными радиолокаторами.

23. Нелинейные радиолокаторы с непрерывным режимом работы.

24. Нелинейные радиолокаторы с импульсным режимом работы.

25. Основы радиоэлектронной борьбы (РЭБ).

26. Методы информационного противоборства.

Раздел II.2 Исследовательский проект

Исследовательский проект должен содержать: титульный лист; оглавление; введение; основную часть; заключение; список использованных источников; приложения (при необходимости).

Титульный лист – первый лист исследовательского проекта, оформляется в соответствии с формой (приложение № 1 к Программе вступительных испытаний).

Исследовательский проект должен отвечать следующим требованиям:

авторская самостоятельность;

полнота исследования;

внутренняя логическая связь, последовательность изложения;

грамотное изложение на русском литературном языке;

высокий теоретический уровень.

Требования к оформлению исследовательского проекта

Исследовательский проект оформляется на листах белого цвета формата А4 с размерами полей: сверху – 20 мм, снизу – 20 мм, справа – 15 мм, слева – 30 мм. Шрифт Times New Roman, кегель (шрифт) –14, через полтора интервала.

Текст исследовательского проекта следует, цвет шрифта черный, выравнивание по ширине.

Объем исследовательского проекта должен составлять не более 35 страниц напечатанного текста.

Защита исследовательского проекта проводится экзаменационной комиссией по программам подготовки научных и научно-педагогических

кадров в аспирантуре, по научной специальности (далее – комиссия) согласно утвержденному расписанию.

Процедура защиты исследовательского проекта включает в себя:

- доклад поступающего (предусматривается не более 8 минут на доклад);

- вопросы членов комиссии по исследовательскому проекту и докладу поступающего (при ответах на вопросы поступающий имеет право пользоваться исследовательским проектом).

Доклад должен включать в себя: обоснование избранной темы; описание цели и задач исследовательского проекта; объект и предмет исследования; круг рассматриваемых проблем и методы их решения; результаты анализа практического материала и их интерпретацию; конкретные рекомендации по совершенствованию разрабатываемой темы. В заключительной части доклада отражается значимость полученных результатов и даются общие выводы.

После выступления автор исследовательского проекта отвечает на вопросы членов комиссии.

Критерии оценивания исследовательского проекта

Критерии	Содержание исследовательского проекта	Защита исследовательского проекта	Итого
Баллы	до 20: - актуальность темы для теории и практики (до 2); - отражение степени разработанности темы (до 3); - логичность изложения основных вопросов (до 2); - наличие дискуссионных вопросов (до 4); - наличие аргументированной точки зрения автора (до 5); - полнота раскрытия темы (до 4)	до 30: - оригинальность и научная обоснованность постановки проблемы и гипотезы предполагаемой темы исследования (до 11); - знание актуальных научных концепций по тематике исследования (до 7); - умение профессионально грамотно и обосновано раскрыть авторскую научную позицию и предложения по теме исследования (до 12)	50

Комиссия при определении результата защиты исследовательского проекта принимает во внимание:

актуальность темы для теории и практики;

отражение степени разработанности темы;

логичность изложения основных вопросов;

наличие дискуссионных вопросов;

наличие аргументированной точки зрения автора;

полнота раскрытия темы.

На основании этого комиссия выставляет баллы.

Исследовательский проект выполняется на русском языке.

Исследовательский проект должен быть выполнен по тематике профиля научной специальности с указанием кафедры.

III. Учебно-методическое обеспечение

Нормативные правовые акты[1]:

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями).

2. Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

3. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

4. Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

5. Указ Президента Российской Федерации от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы"

6. Постановление Правительства Российской Федерации от 08.02.2018 № 127 “Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации”

[1]) Все нормативные правовые акты с изменениями и дополнениями в редакции на день обращения в информационно-справочную правовую систему.

7. Постановление Правительства РФ от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

8. Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации»

9. Приказ ФСТЭК России от 24 марта 2022 г. N 240/22/1549 «О мерах по повышению защищенности информационной инфраструктуры

10. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

Основная литература:

1. Внуков, А. А. Защита информации: учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022.

2. Газизов, А. Р. Техническая защита информации: учебное пособие / А. Р. Газизов, Д. В. Фатхи. – Ростов-на-Дону: ДГТУ, 2022.

3. Козьминых С.И. Обеспечение комплексной защиты объектов информатизации. Учебное пособие. М.: ЮНИТИ-ДАНА: Закон и право, 2019.

4. Крылов Г.О., Никитина В.Л. Понятийный аппарат информационной безопасности финансово-экономических систем. Энциклопедический словарь - М.: Финансовый университет, 2016.

5. Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации: учебное пособие / Рагозин Ю. Н. - Санкт-петербург: ИЦ Интермедия, 2019.

6. Скрипник, Д. А. Общие вопросы технической защиты информации: учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.

7. Фомичёв, В.М. Криптографические методы защиты информации в 2 ч. Часть Математические аспекты: учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников; под ред. В, М. Фомичёва. —М.: Юрайт, 2017.

8. Хорев, П. Б. Программно-аппаратная защита информации: учебное пособие / П. Б. Хорев. - 3-е изд., испр. и доп. - Москва: ИНФРА-М, 2020.

9. Царегородцев А.В. Техническая защита информации: учебное пособие. – М.: Финансовый университет, 2013.

Дополнительная литература:

1. Актуальные проблемы информационного права. Учебник для вузов. ФГОС 3+. В.И. Авдийский, Г.О. Крылов и др.; под ред. И.Л. Бачило, М.А. Лапиной, М.: Издательство КноРус, 2019.

2. Бекетнова Ю.М. Модели и методы решения аналитических задач финансового мониторинга: монография/ Ю.М. Бекетнова, Г.О. Крылов, С.Л. Ларионова. - Москва: Прометей, 2018.

3. Внуков А. А. Защита информации: Учебное пособие - М.: Издательство Юрайт, 2017.

4. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика: учебное пособие / В. Я. Ищейнов. — Москва; Берлин: Директ-Медиа, 2020.

5. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012.

6. Краковский Ю.М., Защита информации: учебное пособие / Ю.М. Краковский - Ростов н/Д: Феникс, 2016.

7. Лупинина О.Р. Основы сетевое безопасности: криптографические алгоритмы и протоколы взаимодействия. Интернет-университет информационных технологий - ИНТУИТ.ру, 2020.

8. Мельников, Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. - 3-е изд., стер. - Москва: ФЛИНТА, 2019.

9. Козьминых С.И. Организационное и правовое обеспечение информационной безопасности. Учебное пособие. Тб., ЮНИТИ-ДАНА

Справедливая Грузия, 2020.

10. Шаньгин В.Ф. Информационная безопасность и защита информации: учебное пособие - Саратов: Профобразование, 2017.

Интернет-ресурсы

Сайт Центрального банка Российской Федерации: www.cbr.ru;

Сайт Федеральной службы по техническому и экспортному контролю: www.fstec.ru;

Сайт Федерального агентства по техническому регулированию и метрологии: www.gost.ru.

Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/ (http://library.fa.ru/files/elibfa.pdf)

Электронно-библиотечная система BOOK.RU http://www.book.ru

Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» http://biblioclub.ru/

Электронно-библиотечная система Znanium http://www.znanium.com

Научная электронная библиотека eLibrary.ru http://elibrary.ru

Электронные ресурсы БИК:

- Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/
- Электронно-библиотечная система BOOK.RU http://www.book.ru
- Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» http://biblioclub.ru/
- Электронно-библиотечная система Znanium http://www.znanium.com
- Электронно-библиотечная система издательства «ЮРАЙТ» https://urait.ru/
- Электронно-библиотечная система издательства Проспект http://ebs.prospekt.org/books
- Деловая онлайн-библиотека Alpina Digital http://lib.alpinadigital.ru/
- Электронная библиотека Издательского дома «Гребенников» https://grebennikon.ru/
- Научная электронная библиотека eLibrary.ru http://elibrary.ru

IV. Примеры тестовых заданий

Тестовое задание 1.

Предметом и объектом защиты в автоматизированных системах являются:

a) предметом защиты информации является информационно телекоммуникационная сеть. Объектом защиты является информация;

b) предметом защиты является информация, хранящаяся, обрабатываемая и передаваемая в информационных системах. Объектом защиты является автоматизированная система;

c) предметом защиты информации является автоматизированная система. Объектом защиты является информация.

Тестовое задание 2.

Под системой защиты информации в автоматизированных системах понимается:

a) применение программно-аппаратных средств, обеспечивающих защиту информационных систем;

b) реализация положений политики безопасности организации;

c) единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в ИС в соответствии с принятой политикой безопасности.

Тестовое задание 3.

Угроза безопасности информации — это:

a) систематические попытки несанкционированного завладения информацией;

b) действия, направленные на получение неавторизованными пользователями доступа к информации;

c) потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации.

Тестовое задание 4.

Перечислите классы потенциальных угроз безопасности информации в автоматизированных системах:

a) случайные, преднамеренные;

b) объективные, субъективные;

c) осуществляемые техническими средствами, осуществляемые программными средствами.

Тестовое задание 5.

Выберите все события, которые относятся к случайным угрозам:

a) стихийные бедствия и аварии;

b) несанкционированный доступ к информации;

c) ошибки пользователей;

d) программные ошибки;

e) вирусные программы;

f) электромагнитные излучения и наводки

Тестовое задание 6.

Процедура, проверяющая, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу, это:

a) идентификация;

b) аутентификация;

c) регистрация;

d) авторизация

Тестовое задание 7.

Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств вычислительной техники или автоматизированных систем, это:

a) несанкционированный доступ к информации;

b) несанкционированная модификация программных структур системы;

c) сбой системы разграничения доступа.

Тестовое задание 8.

Свойство компьютерной системы сохранять работоспособность при отказах отдельных устройств, блоков и схем называется:

a) надежность;

b) отказоустойчивость;

c) целостность;

d) избыточность;

e) адаптивность

Тестовое задание 9.

Присвоение субъектам доступа идентификаторов и/или сравнение предъявляемых идентификаторов с перечнем присвоенных идентификаторов - это:

a) авторизация;

b) аутентификация;

c) идентификация.

Тестовое задание 10.

Выберите все угрозы случайных воздействий:

a) разглашение;

b) предоставление;

c) побочные излучения и наводки;

d) пожар;

e) стихийные действия;

f) ошибки в программах

Тестовое задание 11.

Выберите все угрозы преднамеренных воздействий:

a) разглашение;

b) предоставление;

c) побочные излучения и наводки

d) уничтожение данных;

e) стихийные действия;

f) ошибки в программах

Тестовое задание 12.

Выберите все угрозы утечки информации:

a) разглашение;

b) предоставление;

c) побочные излучения и наводки;

d) уничтожение данных;

e) стихийные бедствия;

f) ошибки в программах.

Тестовое задание 13.

Аспекты обеспечения информационной безопасности;

a) целостность;

b) сопровождаемость;

c) доступность;

d) обслуживаемость;

e) конфиденциальность.

Тестовое задание 14.

Концепция национальной безопасности Российской Федерации - это документ, отражающий:

a) официально принятые взгляды на государственную стратегию в области обеспечения безопасности личности, общества, государства;

b) совокупность официально принятых взглядов на цели и государственную стратегию в области обеспечения безопасности личности, общества, государства от внешних и внутренних угроз политического, экономического, социального, военного, техногенного, экологического, информационного и иного характера с учетом имеющихся ресурсов и возможностей;

c) взгляды государства на цели и стратегию в области обеспечения безопасности личности, общества, государства от внешних и внутренних угроз.

Тестовое задание 15.

Доктрина информационной безопасности - это:

a) основные направления обеспечения информационной безопасности России. Развивает Концепцию национальной безопасности страны применительно к информационной сфере;

b) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности России, Развивает Концепцию национальной безопасности страны применительно к информационной сфере;

c) официальные взгляды на цели и основные направления обеспечения информационной безопасности России. Развивает Концепцию национальной безопасности страны.

Тестовое задание 16.

Механизм управления доступом к информации, при котором права доступа задаются матрицей доступа, элементами которой являются разрешенные права доступа субъекта к объекту называется:

a) мандатный;

b) дискреционный;

c) правовой.

Тестовое задание 17.

Под резервированием механизмов защиты понимают:

a) последовательное включение в систему защиты отказоустойчивых систем;

b) последовательное включение в систему защиты дополнительных механизмов, реализующих те же функции защиты, что и основные механизмы, но иным способом и средствами;

c) включение в систему защиты надежных механизмов, реализующих те же функции защиты.

Тестовое задание 18.

Коэффициент защищенности автоматизированной системы показывает:

a) относительное уменьшение риска в защищенной системе по сравнению с незащищенной системой;

b) относительное увеличение риска в незащищенной системе по сравнению с защищенной системой;

c) риски в защищенной системе по сравнению с незащищенной системой

Тестовое задание 19.

Проектирование системы защиты информации осуществляется в следующей последовательности:

a) проектирование системы защиты (исходный вариант); анализ защищенности на основе статистических данных, полученных в процессе эксплуатации системы защиты; модификация «узких мест» системы защиты; анализ защищенности на основе статистических данных; модификация «узких мест»;

b) проектирование системы защиты (исходный вариант); модификация «узких мест» системы защиты; анализ защищенности на основе статистических данных; модификация «узких мест»;

c) проектирование системы защиты (исходный вариант); анализ защищенности на основе статистических данных, полученных в процессе эксплуатации системы защиты; модификация «узких мест» системы защиты.

Тестовое задание 20.

Выберите механизмы защиты информации в автоматизированных системах:

a) механизмы авторизации;

b) механизмы идентификации;

c) механизмы управления доступом к ресурсам;

d) механизмы контроля целостности;

e) механизмы регистрации (аудита).

Тестовое задание 21.

Каналы, которые относятся к специально создаваемым каналам утечки

информации:

a) побочные электромагнитные излучения;

b) наводки информационных сигналов в линиях электропитания;

c) внедрение закладных устройств;

d) высокочастотное облучение технических средств передачи информации

Тестовое задание 22.

Операции обработки информации средствами вычислительной техники, при которых не возникают побочные электромагнитные излучения:

a) вывод информации на экран монитора;

b) ввод данных с клавиатуры;

c) запись информации на накопители;

d) чтение информации с накопителей; e) передача данных в каналы связи;

e) вывод данных на периферийные печатные устройства;

f) запись данных от сканера на магнитный носитель;

g) во всех перечисленных случаях возникают побочные электромагнитные излучения.

Тестовое задание 23.

Метод управления доступом, при котором возможность для субъекта доступа к объекту определяется сравнением назначенных объекту и субъекту уровней конфиденциальности или уровней уязвимости называется:

a) мандатный;

b) классификационный;

c) дискретный;

d) иерархический.

Тестовое задание 24.

Критерии оценки надежности систем защиты информации:

a) время наработки на отказ;

b) пропускная способность данных по каналам передачи;

c) время устранения соответствующего канала НСД к информации;

d) время внедрения на защищаемый объект исправленной версии системы защиты; e) время передачи информации по запросу пользователя;

e) интенсивность отказов системы.

Задание 25.

Режим резервирования системы защиты дополнительными механизмами дополнительный механизм защиты настроен, но не включен, называется:

a) горячий резерв;

b) активный горячий резерв;

c) пассивный горячий резерв;

d) активный холодный резерв;

e) пассивный холодный резерв.

Задание 26.

Скрытые угрозы информации:

a) некорректность реализации механизма защиты;

b) нерегламентированные действия пользователя;

c) некорректность (противоречивость) возможных настроек механизмов защиты;

d) неполнота покрытия доступа к информации защиты;

e) собственные программы пользователя;

f) ошибки и закладки в ПО.

Тестовое задание 27.

Уровень системы регистрации (аудита), на котором выполняется мониторинг корректности функционирования разграничительных механизмов защиты:

a) первый;
b) второй;
c) нулевой.

Тестовое задание 28.

Уровень системы регистрации (аудита), на котором фиксируются все действия, связанные как с правомерными, так и неправомерными попытками доступа пользователя к ресурсам защищаемого объекта:

a) первый;
b) второй;
c) нулевой.

Тестовое задание 29.

Варианты архитектур системы защиты:

a) распределенная архитектура;
b) централизованная архитектура;
c) централизованно-распределенная архитектура; ё) архитектура звезды;
e) архитектура многогранника.

Тестовое задание 30.

Программный модуль, обеспечивающий маскирующее кодирование (шифрование) и передачу сигналов управления, сигналов синхронизации между локальными и удаленными модулями сетевой системы защиты:

a) сетевой агент;
b) сетевой менеджер;
c) сетевая подсистема;
d) модуль управления локальной базой данных.

Тестовое задание 31.

Модуль сетевой системы защиты, осуществляющий предварительную обработку локальных системных журналов:

a) сетевой агент;
b) сетевой менеджер;
c) сетевая подсистема;

d) модуль управления локальной базой данных;

e) e) модуль центральной базы данных.

Тестовое задание 32.

Идентификация пользователя в автоматизированной системе заключается в:

a) вводе имени;

b) вводе имени и пароля;

c) вводе пароля;

d) сканировании паспортных данных.

Тестовое задание 33.

Аутентификация пользователя в автоматизированной системе заключается в:

a) проверке подлинности идентификации;

b) регистрации в системе пользователя;

c) вводе пароля;

д) вводе имени и пароля.

Тестовое задание 34.
Явные угрозы преодоления парольной защиты:

a) хищение носителя;

b) снифер клавиатуры;

c) подбор пароля;

d) модификация учетных данных на защищаемом обънете;

e) сброс пароля.

Тестовое задание 35.

Дискреционная модель безопасности является механизмом:

a) управления доступом;

b) усиления парольной защиты;

c) контроля целостности;

d) хеширования парольной информации.

Творческая часть

Написать эссе на следующие темы:

1. Обеспечение информационной безопасности в финансово-кредитной организации». Привести примеры потенциальных угроз безопасности, описать перечень мер и средств противодействия угрозам.

2. Способы нарушения конфиденциальности, целостности и доступности информации. Привести примеры таких нарушений.

3. На конкретных нормативные правовых актах дайте характеристику правовых и организационных основ обеспечения информационной безопасности.

4. Приведите примеры организации информационной безопасности защищенного помещения.

5. Дайте характеристику основных уязвимостей программно-аппаратных средств

6. Перечислите основные методы и средства технической защиты информации и их особенности в банковской сфере.

7. Утечка информации от вспомогательной аппаратуры и кабелей, проходящих через помещение. Привести примеры.

8. Дайте характеристику методов пассивной защиты от утечки по электромагнитному каналу.

9. Опишите модель несанкционированного съема информации с помощью радиозакладок.

10. Дайте характеристику методов пассивной защиты от утечки по электромагнитному каналу.

V. Оценка результатов сдачи вступительных испытаний

Вступительное испытание оценивается из расчета 100 баллов:
компьютерное тестирование – до 50 баллов;

защита исследовательского проекта оценивается до 50 баллов и результаты защиты заносятся в ведомость заседания комиссии.

В случае возникновения спорной ситуации при равном числе голосов председательствующий обладает правом решающего голоса.

Общее время выполнения компьютерного тестирования по вступительному испытанию составляет 50 минут.

Время собеседования по исследовательскому проекту составляет 15-20 минут.

Приложение № 1
к Программе

ФОРМА
титульного листа исследовательского проекта

Федеральное государственное образовательное бюджетное учреждение высшего образования «Финансовый университет при Правительстве Российской Федерации»

Исследовательский проект
на тему «_____»
(название темы)

Научная специальность _____ _____
(шифр) *(наименование)*

Кафедра _____
(наименование)

Выполнил:
Ф.И.О.

_____
(личная подпись)

Москва – 202___