Федеральное государственное образовательное бюджетное учреждение

высшего образования

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ**

**ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**

**(Финансовый университет)**

**ПРОГРАММА**

вступительного испытания

для поступающих на обучение по программе подготовки

научно-педагогических кадров в аспирантуре

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Москва 2020

ОГЛАВЛЕНИЕ

[1. Общие положения 3](#_Toc528054659)

[2. Содержание программы вступительного испытания 3](#_Toc528054660)

[3. Учебно-методическое и информационное обеспечение 7](#_Toc528054661)

[4. Примеры заданий 8](#_Toc528054662)

[5. Критерии оценивания вступительного испытания 19](#_Toc528054663)

**Составители:**

Заместитель заведующего кафедрой "Информационная безопасность" по научной работе д.т.н. Козьминых С.И.

Заместитель заведующего кафедрой "Информационная безопасность" по учебно-методической работе к.т.н. Оладько В.С.

Профессор кафедры "Информационная безопасность", д.ф-м.н., профессор Крылов

* 1. Общие положения

Программа вступительного испытания «Информационная безопасность» предназначена для лиц, имеющих документы государственного образца о высшем образовании уровня специалист или магистр и поступающих по программе подготовки научно-педагогических кадров в аспирантуре по направлению 10.06.01 «Информационная безопасность».

Целью вступительных испытаний является 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».

Задачами вступительных испытаний являются оценка уровня подготовленности поступающего и сформированности соответствующих профессиональных компетенций для освоения основной образовательной программы аспирантуры по указанному направлению.

* 1. Содержание программы вступительного испытания

**Основные понятия и принципы теории информационной безопасности**

1. Угрозы информационной безопасности.
2. Виды информации, методы и средства обеспечения информационной безопасности.
3. Методы нарушения конфиденциальности, целостности и доступности информации.
4. Основы комплексного обеспечения информационной безопасности.
5. Модели, стратегии и системы обеспечения информационной безопасности.
6. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
7. Лицензирование и сертификация в области защиты информации.
8. Правовые основы защиты информации.
9. Организационные основы защиты информации.

**Организация ЭВМ и вычислительных сетей**

1. Локальные и глобальные вычислительные сети, типовые конфигурации, маршрутизация.
2. Основные протоколы обмена данными в вычислительных сетях.
3. Системы управления базами данных, реляционная, иерархическая и сетевая модели, распределенные БД.
4. Деревья и графы, их представление в ЭВМ, обходы графов.
5. Алгоритмы на графах, выделение компонент связности.
6. Кратчайшие пути в графе, минимальный остов графа.
7. Задача сортировки и основные алгоритмы сортировки.
8. Поиск информации методом хеширования.
9. Контрольно-испытательные и логико- аналитические методы анализа безопасности программ.
10. Методы и средства хранения ключевой информации в ЭВМ.
11. Защита программ от изучения, защита от изменения, контроль целостности.
12. Защита от разрушающих программных воздействий.

**Криптографическая защита информации**

1. Шифры замены и перестановки, их свойства, композиции шифров.
2. Криптостойкость шифров, основные требования к шифрам.
3. Теоретическая стойкость шифров, совершенные и идеальные шифры.
4. Блоковые шифры.
5. Потоковые шифры.
6. Криптографические хеш-функции, их свойства и использование в криптографии.
7. Методы получения случайных последовательностей, их использование в криптографии.
8. Системы шифрования с открытыми ключами.
9. Криптографические протоколы.
10. Протоколы распределения ключей.
11. Протоколы идентификации.
12. Парольные системы разграничения доступа.
13. Цифровая подпись.
14. Стойкость систем с открытыми ключами.

**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.

**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 мощной офисной аппаратуры.
12. Упрощенная методика определения дальности, на которой возможен перехват ПЭМИ.
13. Утечка информации от вспомогательной аппаратуры и кабелей, проходящих через помещение.
14. Привести примеры.
15. Несанкционированный съем информации с помощью радиозакладок.
16. Достоинства радиозакладок.
17. Основные характеристики радиозакладок.
18. Прослушивание информации от пассивных закладок.
19. Достоинства и недостатки.
20. Структурная схема полуактивного микрофона.
21. Приемники информации с радиозакладок.
22. Деконспирационные признаки радиозакладок.
23. Методы пассивной защиты от утечки по электромагнитному каналу.
24. Технические средства для поиска работающих радиозакладок.
25. Поиск радиозакладок нелинейными радиолокаторами.
26. Нелинейные радиолокаторы с непрерывным режимом работы.
27. Нелинейные радиолокаторы с импульсным режимом работы.
28. Основы радиоэлектронной борьбы (РЭБ).
29. Основы информационного противоборства.
30. Проблемы деанонимизации в теневом интернете.
31. Использование распределенных реестров и технологии блокчейн в задачах информационной безопасности
    1. **Учебно-методическое и информационное обеспечение**

Основная литература

* + 1. Доктрина информационной безопасности Российской Федерации. Утверждена

Указом Президента Российской Федерации от 5 декабря 2016 г. №646

* + 1. Крылов Г.О., Никитина В.Л. Понятийный аппарат информационной безопасности финансово-экономических систем. Энциклопедический словарь - М.: Финансовый университет, 2016.
    2. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для вузов. - М.: Издательский центр «Академия», 2013.
    3. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. - М.: Высшая школа экономики, 2011.
    4. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: ДМК Пресс, 2012.
    5. Фомичёв, В.М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников; под ред. В. М. Фомичёва. — М.: Юрайт, 2017.
    6. Фомичёв, В. М. Криптографические методы защиты информации. В 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под ред. В. М. Фомичёва. — М.: Юрайт, 2016.
    7. 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.: JUSTITIA, 2016

Дополнительная литература

1. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. Стандарт третьего поколения. Учебник для вузов - [Спб: Питер, 2017](https://www.chitai-gorod.ru/search/books/?AUTHOR=%D0%EE%E4%E8%F7%E5%E2+%DE.&SECTION_ID=all)
2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы
3. информационной безопасности: учебное пособие для вузов. - М.: Горячая линия- телеком, 2006.
4. Гатчин Ю.А., Климова Е.В. Основы информационной безопасности - Спб: СПбГУ ИТМО, 2009.
5. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Технические средства и методы защиты информации: учебник для вузов. - М.: Машиностроение, 2009.
6. Ленков С.В., Перегудов Д.А. Методы и средства защиты информации. В 2-х

томах. - М.: Арий, 2009 г.

1. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и

средства. - М.: ДМК Пресс, 2008.

1. Сычев Ю.Н. Основы информационной безопасности. - М.: Евразийский открытый институт, 2010.
2. Крылов Г.О., Ларионова С.Л., Никитина В.Л. Базовые понятия информационной безопасности. Учебное пособие. - М.: РУСАЙНС, 2016
   1. **Примеры заданий**

**Задание 1.**

Предметом и объектом защиты в автоматизированных системах являются:

1. Предметом защиты информации является информационно-телекоммуникационная сеть. Объектов защиты является информация.
2. Предметом защиты является информация, хранящаяся, обрабатываемая и передаваемая в информационных системах. Объектом защиты является автоматизированная система.
3. Предметом защиты информации является автоматизированная система. Объектов защиты является информация.

**Задание 2.**

Под системой защиты информации в автоматизированных системах понимается:

1. применение программно-аппаратных средств, обеспечивающих защиту информационных систем
2. реализация положений политики безопасности организации
3. единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в ИС в соответствии с принятой политикой безопасности

**Задание 3.**

Угроза безопасности информации -это:

1. систематические попытки несанкционированного завладения информацией
2. действия, направленные на получение неавторизованными пользователями доступа к информации
3. потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации

**Задание 4.**

Перечислите классы потенциальных угроз безопасности информации в автоматизированных системах:

1. случайные, преднамеренные
2. объективные, субъективные
3. осуществляемые техническими средствами, осуществляемые программными средствами

**Задание 5.**

Выберите все события, которые относятся к случайным угрозам:

1. стихийные бедствия и аварии
2. несанкционированный доступ к информации
3. ошибки пользователей
4. программные ошибки
5. вирусные программы
6. электромагнитные излучения и наводки

**Задание 6.**

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

1. идентификация
2. аутентификация
3. регистрация
4. авторизация

**Задание 7.**

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

1. несанкционированный доступ к информации
2. несанкционированная модификация программных структур системы
3. сбой системы разграничения доступа

**Задание 8.**

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

1. надежность
2. отказоустойчивость
3. целостность
4. избыточность
5. адаптивность

**Задание 9.**

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

1. авторизация
2. аутентификация
3. идентификация

**Задание 10.**

Выберите все угрозы случайных воздействий

1. разглашение
2. предоставление
3. побочные излучения и наводки
4. пожар
5. стихийные действия
6. ошибки в программах

**Задание 11.**

Выберите все угрозы преднамеренных воздействий

1. разглашение
2. предоставление
3. побочные излучения и наводки
4. уничтожение данных
5. стихийные действия
6. ошибки в программах

**Задание 12.**

Выберите все угрозы утечки информации

1. разглашение
2. предоставление
3. побочные излучения и наводки
4. уничтожение данных
5. стихийные бедствия
6. ошибки в программах

**Задание 13.**

Аспекты обеспечения информационной безопасности:

1. целостность
2. сопровождаемость
3. доступность
4. обслуживаемость
5. конфиденциальность

**Задание 14.**

Концепция национальной безопасности Российской Федерации – это документ, отражающий …

1. официально принятые взгляды на государственную стратегию в области обеспечения безопасности личности, общества, государства
2. 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
3. взгляды государства на цели и стратегию в области обеспечения безопасности личности, общества, государства от внешних и внутренних угроз

**Задание 15.**

Доктрина информационной безопасности – это …

1. основные направления обеспечения информационной безопасности России. Развивает Концепцию национальной безопасности страны применительно к информационной сфере
2. совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности России. Развивает Концепцию национальной безопасности страны применительно к информационной сфере
3. официальные взгляды на цели и основные направления обеспечения информационной безопасности России. Развивает Концепцию национальной безопасности страны

**Задание 16.**

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

1. мандатный
2. дискреционный
3. правовой

**Задание 17.**

Под резервированием механизмов защиты понимают:

1. последовательное включение в систему защиты отказоустойчивых систем
2. последовательное включение в систему защиты дополнительных механизмов, реализующих те же функции защиты, что и основные механизмы, но иным способом и средствами
3. включение в систему защиты надежных механизмов, реализующих те же функции защиты

**Задание 18.**

Коэффициент защищенности автоматизированной системы показывает:

1. относительное уменьшение риска в защищенной системе по сравнению с незащищенной системой
2. относительное увеличение риска в незащищенной системе по сравнению с защищенной системой
3. риски в защищенной системе по сравнению с незащищенной системой

**Задание 19.** *Ларионова С.Л., ТЗ 2-7*

Проектирование системы защиты информации осуществляется в следующей последовательности:

1. 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»
2. проектирование системы защиты (исходный вариант);модификация «узких мест» системы защиты; анализ защищенности на основе статистических данных; модификация «узких мест»
3. проектирование системы защиты (исходный вариант);анализ защищенности на основе статистических данных, полученных в процессе эксплуатации системы защиты; модификация «узких мест» системы защиты

**Задание 20.**

Выберите механизмы защиты информации в автоматизированных системах

1. механизмы авторизации.
2. механизмы идентификации.
3. механизмы управления доступом к ресурсам.
4. механизмы контроля целостности.
5. -механизмы регистрации (аудита).

**Задание 21.**

Каналы, которые относятся к специально создаваемым каналам утечки информации:

1. побочные электромагнитные излучения
2. наводки информационных сигналов в линиях электропитания
3. внедрение закладных устройств
4. высокочастотное облучение технических средств передачи информации

**Задание 22.**

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

1. вывод информации на экран монитора
2. ввод данных с клавиатуры
3. запись информации на накопители
4. чтение информации с накопителей
5. передача данных в каналы связи
6. вывод данных на периферийные печатные устройства
7. запись данных от сканера на магнитный носитель
8. во всех перечисленных случаях возникают побочные электромагнитные излучения

**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 …

1. мандатный
2. классификационный
3. дискретный
4. -иерархический

**Задание 24.**

Критерии оценки надежности систем защиты информации:

1. время наработки на отказ
2. пропускная способность данных по каналам передачи
3. время устранения соответствующего канала НСД к информации
4. время внедрения на защищаемый объект исправленной версии системы защиты
5. время передачи информации по запросу пользователя
6. интенсивность отказов системы

**Задание 25.**

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

1. горячий резерв
2. активный горячий резерв
3. пассивный горячий резерв
4. активный холодный резерв
5. пассивный холодный резерв

**Задание 26.**

Скрытые угрозы информации:

1. некорректность реализации механизма защиты
2. нерегламентированные действия пользователя
3. некорректность (противоречивость) возможных настроек механизмов защиты
4. неполнота покрытия доступа к информации защиты
5. собственные программы пользователя
6. ошибки и закладки в ПО

**Задание 27.**

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

1. первый
2. второй
3. нулевой

**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.

1. первый
2. второй
3. нулевой

**Задание 29.**

Варианты архитектур системы защиты:

1. распределенная архитектура
2. централизованная архитектура
3. централизованно-распределенная архитектура
4. архитектура звезды
5. архитектура многогранника

**Задание 30.**

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

1. Сетевой агент
2. Сетевой менеджер
3. Сетевая подсистема
4. Модуль управления локальной базой данных

**Задание 31.**

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

1. Сетевой агент
2. Сетевой менеджер
3. Сетевая подсистема
4. Модуль управления локальной базой данных
5. Модуль центральной базы данных

**Задание 32.**

Идентификация пользователя в автоматизированной системе заключается в …

1. вводе имени
2. вводе имени и пароля
3. вводе пароля
4. сканировании паспортных данных

**Задание 33.**

Аутентификация пользователя в автоматизированной системе заключается в …

1. проверке подлинности идентификации
2. регистрации в системе пользователя
3. вводе пароля
4. вводе имени и пароля

**Задание 34.**

Явные угрозы преодоления парольной защиты:

1. хищение носителя
2. снифер клавиатуры
3. подбор пароля
4. модификация учетных данных на защищаемом объекте
5. сброс пароля

**Задание 35.**

Дискреционная модель безопасности является механизмом …

1. управления доступом
2. усиления парольной защиты
3. контроля целостности
4. хеширования парольной информации
   1. **Критерии оценивания вступительного испытания**

Вступительное испытание оценивается из расчета 100 баллов.

Общее время выполнения заданий по вступительным испытаниям составляет 50 минут.