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

Департамент информационной безопасности
Факультета информационных технологий и анализа больших данных

УТВЕРЖДАЮ
Проректор по маркетингу и работе
с абитуриентами
_____ С.В. Брюховецкая
«15» 12 2022 г.

ПРОГРАММА

вступительного испытания
для поступающих на обучение по программам подготовки
научных и научно-педагогических кадров в аспирантуре

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ОДОБРЕНО

Протокол заседания
Департамента информационной безопасность
Факультета информационных технологий
и анализа больших данных
от 07.12.2022 № 13

Москва – 2022

ОГЛАВЛЕНИЕ

1. Общие положения

1.1. Программа вступительного испытания «Методы и системы защиты информации, 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».

1.2. 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.

2. Содержание программы вступительного испытания. Основные понятия и принципы теории информационной безопасности

1. Классификация угроз информационной безопасности.

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

3. Способы нарушения конфиденциальности, целостности и доступности информации.

4. Основы комплексного обеспечения информационной безопасности.

5. Методы, модели и стратегии 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 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.

27. Проблемы деанонимизации в теневом интернете;

28. Использование распределенных реестров и технологии блокчейн в задачах информационной безопасности.

3. Учебно-методическое и информационное обеспечение

Основная литература

1. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646.

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

3. Бекетнова Ю.М. Модели и методы решения аналитических задач финансового мониторинга: монография/ Ю.М. Бекетнова, Г.О. Крылов, С.Л. Ларионова. - Москва: Прометей, 2018. – 274 с. - Текст: непосредственный. – То же. - ЭБС Университетская библиотека online. – URL: http://biblioclub.ru/index.php?page=book_red&id=494851&sr=1

4. Козьминых С.И. Обеспечение комплексной защиты объектов информатизации. Учебное пособие. М.: ЮНИТИ-ДАНА: Закон и право, 2019. – 640 с.

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.: Издательство КноРус , 2019.

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.

2. Козьминых С.И. Организационное и правовое обеспечение информационной безопасности. Учебное пособие. Тб., ЮНИТИ-ДАНА Справедливая Грузия, 2020. 309 с.

3. Аникин В.М. Диссертация в зеркале автореферата: методическое пособие для аспирантов и соискателей ученой степени естественно-научных специальностей/ В.М. Аникин. - Москва: Инфра-М, 2019. – 128 с. - ЭБС Znanium.com. - URL: http://znanium.com/catalog/product/1008538 (дата обращения: 17.10.2019). - Текст: электронный.

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

5. Резник С.Д. Аспирант вуза: технологии научного творчества и педагогической деятельности: учебник /С.Д. Резник. – Москва: ИНФРА-М, 2019. – 400 с. - ЭБС Znanium.com. - URL: http://znanium.com/catalog/product/944379 (дата обращения: 17.10.2019). - Текст: электронный.

6. Крылов Г.О., Ларионова С.Л., Никитина В.Л. Базовые понятия информационной безопасности. Учебное пособие. - М.: РУСАЙНС, 2016.

4. Примеры тестовых заданий

Экзаменационный билет состоит из двух частей: тестовой и творческой.

Тестовая часть

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.

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.

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.

Задание 4.

Перечислите классы потенциальных угроз безопасности информации в автоматизированных системах:

a) случайные, преднамеренные;
b) объективные, субъективные;
c) осуществляемые техническими средствами, осуществляемые программными средствами.

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.

Задание 6.

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

a) идентификация;
b) аутентификация;
c) регистрация;
d) авторизация.

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.

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.

Задание 9.

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

a) авторизация;

b) аутентификация;

c) идентификация.

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.

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.

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.

Задание 13.

Аспекты обеспечения информационной безопасности:

a) целостность;

b) сопровождаемость;

c) доступность;

d) обслуживаемость;

e) конфиденциальность.

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.

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.

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.

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.

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.

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.

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).

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.

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;

f) вывод данных на периферийные печатные устройства;

g) запись данных от сканера на магнитный носитель;

h) 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:

a) мандатный;

b) классификационный;

c) дискретный;

d) иерархический.

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;
f) 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.

Задание 27.

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

a) первый;

b) второй;

c) 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:

a) первый;

b) второй;

c) нулевой.

Задание 29.

Варианты архитектур системы защиты:

a) распределенная архитектура;

b) централизованная архитектура;

c) централизованно-распределенная архитектура;

d) архитектура звезды;

e) архитектура многогранника.

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.

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) модуль центральной базы данных.

Задание 32.

Идентификация пользователя в автоматизированной системе заключается в:

a) вводе имени;

b) вводе имени и пароля;

c) вводе пароля;

d) сканировании паспортных данных.

Задание 33.

Аутентификация пользователя в автоматизированной системе заключается в:

a) проверке подлинности идентификации;

b) регистрации в системе пользователя;

c) вводе пароля;

d) вводе имени и пароля.

Задание 34.

Явные угрозы преодоления парольной защиты:

a) хищение носителя;

b) снифер клавиатуры;

c) подбор пароля;

d) модификация учетных данных на защищаемом объекте;

e) сброс пароля.

Задание 35.

Дискреционная модель безопасности является механизмом:

a) управления доступом;
b) усиления парольной защиты;
c) контроля целостности;
d) хеширования парольной информации.

Творческая часть

Пример 1. Написать эссе на тему «Обеспечение информационной безопасности в финансово-кредитной организации». Привести примеры потенциальных угроз безопасности, описать перечень мер и средств противодействия угрозам.

5. Оценка результатов сдачи вступительных испытаний

Вступительное испытание оценивается из расчета 100 баллов и состоит из: 35 тестовых заданий, оцениваемых из расчета 70 баллов (2 балла за тестовое задание) и письменного ответа на вопрос по программе аспирантуры, оцениваемого в 30 баллов в соответствии с критериями оценки, приведенными в таблице 1.

Таблица 1 - Критерии оценки ответа на вопрос

Критерии	Количество баллов
1. Соответствие содержания ответа на вопрос заявленной теме (проблематике)	5
2. Полнота и логичность ответа (использование научной терминологии, понятийно-категориального аппа-	10

рата соответствующей отрасли знания, логичное и доказательное изложение вопроса, знание научных позиций отечественных и\или зарубежных исследователей по данной проблематике)	
3. Аргументированность выводов и положений поступающего при ответе на вопрос	5
4. Наличие в ответе на вопрос четко и грамотно сформулированной позиции (мнения) поступающего (способность представить собственные выводы, привести пример(ы))	10
ИТОГО	30

Общее время выполнения заданий по вступительным испытаниям составляет 90 минут.