Федеральное государственное образовательное бюджетное 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,
ответственный секретарь
приемной комиссии
_____ С.В. Брюховецкая
«____» _____ 2023 г.

ПРОГРАММА

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

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ОДОБРЕНО

Протокол заседания
Совета Департамента
информационной безопасности
Факультета информационных
технологий и анализа больших
данных от 18.12.2023 № 4

Москва – 2023

СОДЕРЖАНИЕ

1. Общие положения 3
2. Содержание программы вступительного испытания 3
3. Учебно-методическое и информационное обеспечение 7
4. Примеры тестовых заданий 9
5. Оценка результатов сдачи вступительных испытаний 20

Составитель: профессор Департамента информационной безопасности Мельников Д.А.

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. Понятие, цели и задачи обеспечения информационной безопасности (доступность, целостность, конфиденциальность, идентифицируемость и гарантированность).

2. Концепции обеспечения информационной безопасности (субъекты, объекты, вспомогательная информация, функциональные и вспомогательные средства).

3. Основные направления обеспечения информационной безопасности (аутентификация, управление доступам, обеспечение неотказуемости, конфиденциальности, целостности и криптографическими ключами, аудит информационной безопасности).

4. Классификация и последствия реализации угроз информационной безопасности (вскрытие, обман, разрушение, узурпация).

5. Теоретические основы аутентификации, классификация способов и средств аутентификации. Различие между процедурами аутентификации и

идентификации.

6. Теоретические основы управления доступом. Функции и классификация схем (моделей) управления доступом, и критерии классификации.

7. Теоретические основы обеспечения неотказуемости. Этапы (фазы) обеспечения неотказуемости. Модель и состав участников системы обеспечения неотказуемости.

8. Теоретические основы, классификация способов и средства обеспечения конфиденциальности.

9. Теоретические основы, классификация способов и средства обеспечения целостности.

10. Теоретические основы аудита информационной безопасности (ИБ) и оповещения об опасности.

11. Теоретические основы обеспечения криптографическими ключами. Модель жизненного цикла криптографического ключа. Основные модели обеспечения криптографическими ключами.

12. Основные технические модели системы обеспечения информационной безопасности (СОИБ). Распределённые службы обеспечения ИБ. Сегменты безопасности. Изолированные ЛВС.

13. Лицензирование и сертификация в области защиты информации.

14. Правовые основы защиты информации. Законодательство и нормативные правовые акты.

15. Организационно-технические основы защиты информации.

Организация информационно-технологических сетей (систем)

1. Общие характеристики организации информационно-технологических систем/сетей (ИТС). Структура, топология и архитектура. Протоколы, интерфейсы и структура сообщений.

2. Методы коммутации и передачи данных в ИТС. Коммутация каналов, сообщений и пакетов. Дейтаграммы и виртуальные каналы.

3. Организация управления потоками данных в ИТС. Способы адресации. Маршрутизация пакетов. Управление потоками. Защита от перегрузок.

4. Протоколы прикладного уровня в ИТС. Протокол виртуального терминала. Передача файлов. Удаленный ввод заданий. Распределенная обработка. Электронная почта. Протоколы обработки графической информации.

5. Административное управление ИТС. Функции. Организация.

6. Интернет-архитектура. Протоколы, интерфейсы и логические модули. Канальные, сетевые и транспортные протоколы.

7. Гипертекстовые информационно-технологические системы. Протоколы HTTP 1.1, HTTP 2.0, HTTP 3, QUIC: основные различия.

8. Принципы построения локальных вычислительных сетей (ЛВС), архитектура и структуры ЛВС. Моноканалы.

9. Организация моноканалов (сетевой адаптер) в ЛВС. Селективный способ коммутации кадров. Свободный доступ с проверкой несущей. Эстафетный доступ.

10. Принципы множественного доступа в беспроводных ЛВС. Радиомульиплексор.

11. Современные стандарты организации ЛВС.

12. Системы управления базами данных. Реляционная, иерархическая и сетевая модели. Распределенные БД.

Криптографические методы защиты информации

1. Симметричные криптографические системы.

2. Асимметричные криптографические системы.

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

4. Криптостойкость шифров, основные требования к шифрам.

5. Теоретическая стойкость шифров, совершенные и идеальные шифры.

6. Блочные и поточные шифры.

7. Криптографические однонаправленные (хеш-) функции, их свойства и использование в СОИБ.

8. Методы формирования случайных последовательностей (чисел), их использование в криптографии.

9. Криптографические протоколы. Цель и задачи, решаемые криптопротоколами.

10. Инфраструктуры открытых ключей (ИОК). Модель и состав ИОК. Центры сертификации и регистрации. Состав сертификата открытого ключа ($СЕРТ_{ОК}$). Атрибутный сертификат ($СЕРТ_{АТ}$).

11. Использование цифровых подписей в кредитно-финансовой сфере. Системы криптовалют на основе технологии «криптосвязки блоков» (*Blockchain*), угрозы и риски ИБ кредитно-финансовых организаций. Система

цифрового рубля.

12. Основные способы распределения и доставки криптографических ключей (симметричные, асимметричные и парольные методы).

13. 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.

14. Понятие доверия в ИТС. Модели доверия и связь доверия с ИБ. Обеспечение доверия в ИТС. Субъективная логика.

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 обнаружения и локализации вредоносных закладных устройств.

6. Методы подавления опасных сигналов акустоэлектрических преобразователей и поверхностных акустических волн.

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

8. Виды контроля эффективности защиты информации.

9. Методы расчёта и инструментального контроля показателей защиты информации.

10. Несанкционированный съём информации с помощью радиозакладок. Технические средства, предназначенные для поиска работающих радиозакладок.

11. Методы пассивной защиты от утечки по электромагнитному каналу.

12. Теория информационного противоборства (войны). Контроль мировых информационных потоков как способ и средство информационного противоборства (войны). Компьютерный шпионаж. Объекты и источники компьютерного шпионажа.

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. Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем: Учебник. – М.: IDO Press, Университетская книга, 2012. ISBN 978-5-4243-0004-2.

3. Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации (в 2-х частях): Учебное пособие. М.: Юрайт. 2016. ISBN 978-5-9916-7089-3.

4. Мельников Д.А. Информационная безопасность открытых систем: Учебник. – М.: ФЛИНТА, Наука, 2013. – 448 с. ISBN 978-5-9765-1613-7.

5. National Institute of Standards and Technology. Introduction to Public Key Technology and the Federal PKI Infrastructure. NIST Special Publication 800-32, 26 February 2001.

6. ITU-T. Recommendation X.810 (ISO/IEC 10181-1: 1996), Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Overview, 1995.

7. ITU-T. Recommendation X.811 (ISO/IEC 10181-2: 1996), Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Authentication Framework, 1995.

8. ITU-T. Recommendation X.812 (ISO/IEC 10181-3: 1996), Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Access Control Framework, 1995.

9. ITU-T. Recommendation X.813 (ISO/IEC 10181-4: 1996), Information Technology – Open Systems Interconnection –Security Frameworks for Open Systems: Non-repudiation Framework, 1995.

10. ITU-T. Recommendation X.814 (ISO/IEC 10181-5: 1996), Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Confidentiality Framework, 1995.

11. ITU-T. Recommendation X.815 (ISO/IEC 10181-6: 1996), Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Integrity Framework, 1995.

12. ITU-T. Recommendation X.509 (ISO/IEC 9594-8, 2016), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, 2016.

13. ISO/IEC, Information technology – Security techniques – Key management – Part 1: Framework. ISO/IEC 11770-1, 2010-12-01.

14. National Institute of Standards and Technology. Underlying Technical Models for Information Technology Security. NIST Special Publication 800-33, December 2001.

Дополнительная литература

1. Анин Б., Петрович А. Радиошпионаж. – М.: Международные отношения, 1996. – 448 с. ISBN 5-7133-0866-9.

2. Мельников Д.А. Системы и сети передачи данных: Учебник. – М.: РадиоСофт, 2015. – 624 с. 978-5-93037-294-6.

3. McNamara J. Secrets of Computer Espionage: Tactics and Countermeasures. John Wiley & Sons, Inc., N.Y., 2003.

4. Будзко В.И., Горбатов В.С., Жуков Ю.И. и Мельников Д.А. К вопросу универсальности технологии «Blockchain» // Проблемы информационной безопасности. Компьютерные системы. – 2019, №1, стр. 45-54. ISSN 2071-8217. URI: http://jisp.ru/o-zhurnale/arxiv-nomerov/.

5. National Institute of Standards and Technology. Blockchain Technology Overview. NISTIR 8202, October 2018. URI: https://doi.org/10.6028/NIST.IR.8202

6. Мельников Д.А., Мельников А. Д. Национальная система доверия на основе инфраструктуры открытых ключей для цифровой экономики Российской Федерации. Монография. – М.: Горячая линия – Телеком, 2023, – 384 с. (ISBN 978-59912-1030-0)

7. Jøsang A. Subjective Logic. A Formalism for Reasoning Under Uncertainty. – Springer International Publishing, Switzerland, 2016. – 337 p. ISBN 978-3-319-42335-7(1). DOI 10.1007/ 978-3319-42337-1.

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

9. 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.

4. Примеры тестовых заданий

Экзаменационный билет состоит из двух частей: тестовой и творческой.

Тестовая часть

Задание 1.

Цель обеспечения информационной безопасности (ИБ):

a) надёжная защита персональных данных и обеспечение их неприкосновенности, предотвращение атак типа «отказ в обслуживании», «маскарад», «повторная передача» и «подмена»;

b) предоставить организации возможность решать все свои финансово-экономические задачи и добиваться определённых результатов в своей основной деятельности с помощью внедрения ИТС в точном соответствии с рисками для организации, связанными с использованием ИТС и взаимодействием со своими партнёрами и потребителями;

c) защита прикладных ИТС от вредоносных программ, предотвращение несанкционированного доступа к защищаемым ресурсам и данным, предотвращение несанкционированного проникновения в охраняемую зону (например, помещения, в которых обрабатывается, храниться, визуализируется и регистрируется конфиденциальная информация).

Задание 2.

Под системой обеспечения ИБ понимается:

a) реализация положений политики информационной безопасности организации;

b) система, объединяющая политику (стратегию) обеспечения ИБ организации, организационные меры, комплексы технических средств (программные и программно-аппаратные), реализующие данную политику и соответствующие технологии защиты информации (ресурсов, активов организации), а также обслуживающий их персонал (включая высшее руководство организации), которая предназначена для снижения (нейтрализации) финансово-экономических рисков организации;

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

Задание 3.

Угроза информационной безопасности – это:

a) систематические попытки несанкционированного завладения информацией;

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

c) потенциальная причина (источник) нежелательного инцидента, который может нанести вред ИТС (СОИБ) или финансово-экономический ущерб организации, и который связан с нарушением целостности, конфиденциальности доступности информации, искажением идентифицируемости субъектов, объектов и процессов, и отсутствием гарантированности и доверия.

Задание 4.

Международный стандарт IETF (RFC 4949) определяет следующие виды последствий реализации угроз:

a) потеря контроля маршрутизации, пропуск сообщений и блокировка прикладной службы;

b) вскрытие, обман, разрушение и захват (узурпация);

c) потеря взаимосвязи между элементами сети и нарушение топологии ИТС;

d) перенаправление и искажение информационных потоков, потеря управления сетевым трафиком;

e) компрометация криптографических ключей;

f) все вышеперечисленные.

Задание 5.

Процедура аутентификации отвечает на вопрос:

a) «как вам здесь?»;

b) «а объект действительно является тем, за кого себя выдаёт?»;

c) «а объект действительно существует, или он придуман?»;

d) «а зачем вы тут?»;

e) все вопросы не относятся к процедуре аутентификации.

Задание 6.

Процедура идентификации отвечает на вопрос:

a) «свой или чужой?»;

b) «вы, кто такой?»;

c) «кто крайний?»;

d) «вы здесь зачем?»;

e) все вопросы не относятся к процедуре идентификации.

Задание 7.

Принципы, используемые при аутентификации, следующие:

a) что-нибудь известно;

b) чем-нибудь владеют;

c) некоторые неизменные характеристики;

d) признание такого третьего объекта (ДТС), который бы подтвердил результаты процедуры аутентификации;

e) контекст (дополнительная информация).

f) все вышеперечисленные.

Задание 8.

Интернет-архитектура включает:

a) 3 уровня;

b) 4 уровня;

c) 5 уровней;

d) 6 уровней;

e) 7 уровней.

Задание 9.

Архитектура ЛВС включает:

a) 3 уровня;

b) 4 уровня;

c) 5 уровней;

d) 6 уровней;

e) 7 уровней.

Задание 10.

Интранет-архитектура (ЛВС, реализующая Интернет-архитектуру) включает:

a) 3 уровня;

b) 4 уровня;

c) 5 уровней;

d) 6 уровней;

e) 7 уровней.

Задание 11.

Основная цель УД заключается в:

a) обеспечении надёжной доставки пакетов, включая их идентификацию и корректную маршрутизацию;

b) минимизации зависимости от «ненадежных коммутаторов пакетов» (маршрутизаторов);

c) парировании угроз, связанных с несанкционированными операциями (действиями), которые затрагивают функционирование компьютеров или систем связи;

d) организации защищённых двунаправленных виртуальных соединений (например, шифрование пакетов) между удалёнными процессами.

Задание 12.

Термин «доверенная третья сторона» (ДТС, trusted third party) используется для определения …

a) удостоверяющего центра, выпускающего сертификаты открытых ключей и вспомогательные атрибутные сертификаты;

b) центра регистрации;

c) центра распределения вспомогательной информации (например, криптографических ключей);

d) центра безопасности или его представителя, которому доверяют обе взаимодействующие стороны, относительно его деятельности по обеспечению безопасности.

Задание 13.

Концептуальные основы обеспечения ИБ включают:

a) аутентификацию;

b) управление доступом;

c) обеспечение неотказуемости;

d) обеспечение конфиденциальности;

e) обеспечение целостности;

f) аудит безопасности и оповещение об опасности;

g) обеспечение криптографическими ключами;

h) всё вышеперечисленное.

Задание 14.

Стратегия национальной безопасности Российской Федерации – это:

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

b) базовый документ стратегического планирования, определяющий национальные интересы и стратегические национальные приоритеты Российской Федерации, цели и задачи государственной политики в области обеспечения национальной безопасности и устойчивого развития Российской Федерации на долгосрочную перспективу;

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) система официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере;

b) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности России;

c) основные направления обеспечения информационной безопасности России.

Задание 16.

Критерием классификации схем (моделей) управления доступом является:

a) место размещения прав доступа инициатора к целевому объекту;

b) наличие систем аутентификации и идентификации;

c) наличие таблиц, содержащих права доступа инициатора к целевому объекту;

d) место размещения биометрических параметров подлинности инициатора.

Задание 17.

Какие модели (схемы) управления доступом определяет Международный стандарт ITU-T X.812 от 1995 (ISO/IEC 10181-3: 1996):

a) на основе списков доступа;

b) компетентностная (мандатная);

c) на основе меток безопасности;

d) контекстно-зависимую модель (схему);

e) все вышеперечисленные.

Задание 18.

Вспомогательная информация для обеспечения ИБ (*security information*) включает:

a) правила (положения) политики обеспечения ИБ;

b) информацию, необходимую для функционирования определённых служб обеспечения ИБ;

c) информацию, необходимую для реализации способов обеспечения ИБ;

d) всё вышеперечисленное.

Задание 19.

К криптографическим проверочным суммам относятся:

a) криптоконверты;

b) цифровые подписи;

c) цифровые отпечатки;

d) всё вышеперечисленное.

Задание 20.

В модели (схеме) управления доступом на основе списков доступа информация о правах доступа инициатора располагается:

a) в базе данных доверенной третьей стороны;

b) на стороне инициатора;

c) на стороне целевого объекта;

d) в базе данных провайдера службы сертификации;

e) на стороне злоумышленника.

Задание 21.

Искусственно созданными каналами утечки информации являются:

a) поверхностные акустические волны;

b) побочные электромагнитные излучения;

c) наводки информационных сигналов в линиях электропитания;

d) каналы утечки, создаваемые вредоносными закладными устройствами (типа «троянский конь»);

e) высокочастотное облучение технических средств передачи информации (принцип интермодуляции).

Задание 22.

Основными функциями, реализуемыми в процессе УД, являются:

a) функции вычисления криптографической проверочной суммы и цифровой подписи;

b) однонаправленная функция и функция вычисления цифрового отпечатка;

c) функции принуждения и принятия решения;

d) аутентификация и идентификация инициаторов;

e) все вышеперечисленные.

Задание 23.

Компетентностная (мандатная) схема УД наиболее приемлема там, где:

a) имеет место несколько целевых объектов;

b) имеет место несколько инициаторов или групп инициаторов;

c) имеет место много инициаторов, запрашивающих доступ ко многим целевым объектам;

d) всё вышеперечисленное.

Задание 24.

Форма реализации служба обеспечения неотказуемости следующая:

a) неотказуемость с доказательством источника и неотказуемость с доказательством доставки;

b) неотказуемость с подтверждением ЭЦП и неотказуемость с доказательством ретрансляции;

c) неотказуемость с доказательством доставки и неотказуемость с подтверждением приёма;

d) неотказуемость с доказательством ретрансляции и неотказуемость с подтверждением источника;

e) все вышеперечисленные.

Задание 25.

Конфиденциальность – это свойство информации, которое:

a) обеспечивает её криптографическую привязку к взаимодействующей стороне;

b) обеспечивает её недоступность или нераскрываемость для неавторизованных пользователей, объектов и процессов;

c) предотвращает её изменение или разрушение неавторизованным способом;

d) обеспечивает скрытый доступ к защищаемому ресурсу;

e) всё вышеперечисленное.

Задание 26.

Продолжите фразу «целостность данных определяется …»:

a) количеством защищённых символов;

b) надёжностью используемых криптоалгоритмов;

c) семантическим содержанием данных;

d) постоянством смыслового значения данных;

e) количеством защищённых файлов.

Задание 27.

Приём запроса на получение $СЕРТ_{ОК}$ должен осуществляться только путём:

a) отправки информации с запросом на получение $СЕРТ_{ОК}$ заказным письмом;

b) отправки информации с запросом на получение $СЕРТ_{ОК}$ обычным письмом;

c) персонального вручения информации с запросом на получение $СЕРТ_{ОК}$;

d) отправки информации с запросом на получение $СЕРТ_{ОК}$ с помощью службы электронной почты;

e) отправки информации с запросом на получение $СЕРТ_{ОК}$ с помощью курьерской службы.

Задание 28.

Продолжите фразу «Аудит информационной безопасности включает …»:

a) процедуры обеспечения целостности, конфиденциальности, доступности информации, идентифицируемости и гарантированности;

b) обнаружение, отбор и регистрацию различных событий, которые тем или иным образом связаны с обеспечением (состоянием) безопасности (событием безопасности), для аудиторской проверки обеспечения (состояния) безопасности и анализ таких событий;

c) процедуры обеспечения недоступности или нераскрываемости данных для незарегистрированных пользователей, объектов и процессов;

d) процедуры криптографической защиты данных, обмена, доставки и формирования криптографических ключей;

e) всё вышеперечисленное.

Задание 29.

Одним из видов реализации угроз ИБ является «мистификация» (spoof), которая приводит к:

a) узурпации (захвату);

b) обману;

c) вскрытию;

d) разрушению;

e) всему вышеперечисленному.

Задание 30.

Одним из видов реализации угроз ИБ является «перегрузка» (overload), которая приводит к:

a) разрушению;

b) обману;

c) вскрытию;

d) узурпации (захвату);

e) всему вышеперечисленному.

Задание 31.

В открытых ИТС (СОИБ) сигнал оповещения об опасности (или сигнал опасности) представляет собой …

a) звуковой сигнал типа «сирена», оповещающий о необходимости покинуть своё рабочее место и переместиться в безопасную зону;

b) светозвуковой сигнал типа «сигнальная ракета», оповещающий о необходимости покинуть своё рабочее место и переместиться в зону безопасности;

c) сообщение, следующее после обнаружения события безопасности, которое классифицировано как событие, приводящее к нарушению безопасности и возникновению условий для формирования и подачи сигнала опасности;

d) сигнал пожарной тревоги, оповещающий о необходимости покинуть своё рабочее место и переместиться в безопасную зону.

Задание 32.

Модель сертификации открытого ключа включает следующие логические объекты:

a) удостоверяющий центр (или центр сертификации), центр регистрации ключей и пользователь;

b) удостоверяющий центр (или центр сертификации), центр эксплуатации и сопровождения службы Единого каталога, модуль генерации ключей, центр регистрации ключей и пользователь;

c) модуль генерации ключей, центр регистрации ключей и пользователь;

d) центр эксплуатации и сопровождения службы Единого каталога, модуль генерации ключей, центр регистрации ключей и пользователь;

e) центр распределения ключей, модуль генерации ключей, центр регистрации ключей и пользователь;

f) центр эксплуатации и сопровождения службы Единого каталога, модуль генерации ключей и пользователь.

Задание 33.

Аутентификацией называется:

a) проверка цифровой подписи;

b) регистрация в системе пользователя;

c) процедура подтверждения подлинности;

d) ввод имени и пароля;

e) проверка документов (например, идентификационный номер налогоплательщика);

f) всё вышеперечисленное.

Задание 34.

Схема УД на основе списков доступа наиболее приемлема там, где:

a) имеет место несколько целевых объектов;

b) имеет место несколько инициаторов или групп инициаторов;

c) имеет место много инициаторов, запрашивающих доступ ко многим целевым объектам;

d) всё вышеперечисленное.

Задание 35.

Основной угрозой службе обеспечения неотказуемости является …

a) компрометация криптографических ключей;

b) компрометация доказательства;

c) фальсификация доказательства;

d) злонамеренная модификация криптографических ключей;

e) все вышеперечисленные.

Творческая часть

Пример 1. Написать эссе на тему «Обеспечение информационной безопасности в кредитно-финансовой организации». Привести примеры потенциальных угроз безопасности, описать перечень методов, способов и средств парирования (нейтрализации) угроз.

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 правильное решение тестового задания) и письменного ответа на вопрос по программе аспирантуры, оцениваемого в 30 баллов в соответствии с критериями оценки, приведёнными 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 аппарата соответствующей отрасли знания, логичное и доказательное изложение вопроса, знание научных позиций отечественных и\или зарубежных исследователей по данной проблематике)	10
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.