МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

УТВЕРЖДАЮ
Первый проректор-проректор
по научной работе

_____ А.В. Коржов

«____»_____2022 г.

**ПРОГРАММА**

кандидатского экзамена по специальной дисциплине:

Научная специальность: *2.3.6. Методы и системы защиты информации, информационная безопасность*

Разработчики:

*1. _____ Соколов А.Н., кандидат технических наук, доцент, заведующий кафедрой «Защита информации»*

*2. _____ Зюляркина Н.Д., доктор физико-математических наук, доцент, профессор кафедры «Защита информации»*

Челябинск 2022 г.

## 1. Перечень тем для подготовки к кандидатскому экзамену

Экзамен состоит из двух частей: общая часть по методам и системам защиты информации и специальная часть по информационной безопасности.

Общая часть по методам и системам информации содержит основной материал на темы – законодательные и правовые основы защиты компьютерной информации информационных технологий, проблемы защиты информации в информационных системах, содержание системы средств защиты компьютерной информации в информационных системах.

Специальная часть по информационной безопасности включает вопросы, внесенные в курсы и спецкурсы по темам – симметричные и асимметричные криптосистемы, методы идентификации и проверки подлинности пользователей компьютерных систем, защита компьютерных систем от удаленных атак через сеть Internet, существующие аппаратно-программные средства криптографической защиты компьютерной информации серии КРИПТОН, методы защиты программ от изучения и разрушающих программных воздействий, комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.

Раздел 1.Общая часть по методам и системам защиты информации

1. Законодательные и правовые основы защиты компьютерной информации информационных технологий. Безопасность информационных ресурсов и документирование информации; государственные информационные ресурсы; персональные данные о гражданах; права на доступ к информации; разработка и производство информационных систем; вычислительные сети и защита информации; нормативно-правовая база функционирования систем защиты информации; компьютерные преступления и особенности их расследования; российское законодательство по защите информационных технологий; промышленный шпионаж и законодательство, правовая защита программного обеспечения авторским правом.

2. Проблемы защиты информации в информационных системах. Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах; основные задачи обеспечения безопасности информации в информационных системах; защита локальных сетей и операционных систем; интеграция систем защиты; Internet в структуре информационно-аналитического обеспечения информационных систем; рекомендации по защите информации в Internet.

3. Содержание системы средств защиты компьютерной информации в информационных системах. Защищенная информационная система и система

защиты информации; принципы построения систем защиты информации и их основы; законодательная, нормативно-методическая и научная база системы защиты информации.

4. Требования к содержанию нормативно-методических документов по защите информации; научно-методологический базис, стратегическая направленность и инструментальный базис защиты информации; структура и задачи (типовой перечень) органов, выполняющих защиту информации.

5. Организационно-правовой статус службы информационной безопасности; организационно-технические и режимные меры; политика безопасности: организация секретного делопроизводства и мероприятий по защите информации; программно-технические методы и средства защиты информации; программно-аппаратные методы и средства ограничения доступа к компонентам компьютера; типы несанкционированного доступа и условия работы средств защиты; вариант защиты от локального несанкционированного доступа и от удаленного ИСПДн. Средства защиты, управляемые модемом, надежность средств защиты.

Раздел 2. Специальная часть по информационной безопасности

1. Традиционные симметричные криптосистемы. Основные понятия и определения; шифры перестановки; шифр перестановки «скитала»; шифрующие таблицы; применение магических квадратов; шифры простой замены; полибианский квадрат; система шифрования Цезаря; система шифрования Вижинера; шифр «двойной квадрат» Уитстона; одноразовая система шифрования; шифрование методом Вернама; роторные машины; шифрование методом гаммирования; методы генерации псевдослучайных последовательностей чисел.

2. Применение симметричных криптосистем для защиты компьютерной информации в информационных системах. Американский стандарт шифрования данных DES; основные режимы работы алгоритма DES; отечественный стандарт шифрования данных; режим простой замены; режим гаммирования; режим гаммирования с обратной связью; режим выработки имитовставки; блочные и поточные шифры.

3. Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах. Концепция криптосистемы с открытым ключом; однонаправленные функции; криптосистема шифрования данных RSA (процедуры шифрования и расшифрования в этой системе); безопасность и быстродействие криптосистемы RSA; схема шифрования Полига–Хеллмана; схема шифрования эль-Гамаля, комбинированный метод шифрования.

4. Методы идентификации и проверки подлинности пользователей компьютерных систем. Основные понятия и концепции; идентификация и механизмы подтверждения подлинности пользователя; взаимная проверка

подлинности пользователей; протоколы идентификации с нулевой передачей знаний; упрощенная схема идентификации с нулевой передачей знаний; проблема аутентификации данных и электронная цифровая подпись; однонаправленные хэш-функции; алгоритм безопасного дешифрования SHA; однонаправленные хэш-функции на основе симметричных блочных алгоритмов; отечественный стандарт хэш-функции; алгоритм цифровой подписи RSA; алгоритм цифровой подписи эль-Гамаля (EGSA); алгоритм цифровой подписи DSA; отечественный стандарт цифровой подписи.

5. Защита компьютерных систем от удаленных атак через сеть Internet. Режим функционирования межсетевых экранов и их основные компоненты; маршрутизаторы; шлюзы сетевого уровня; усиленная аутентификация; основные схемы сетевой защиты на базе межсетевых экранов; применение межсетевых экранов для организации виртуальных корпоративных сетей; программные методы защиты.

6. Существующие аппаратно-программные средства криптографической защиты компьютерной информации серии КРИПТОН. Основные элементы средств защиты сети от несанкционированного доступа; устройства криптографической защиты данных; контроллер смарт-карт SCAT-200; программно-аппаратная система защиты от несанкционированного доступа (НСД) КРИПТОН-ВЕТО; защита от НСД со стороны сети; абонентское шифрование и ЭЦП; шифрование пакетов; аутентификация; защита компонентов ЛВС от НСД; защита абонентского пункта, маршрутизаторов и устройств контроля; технология работы с ключами.

7. Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Классификация способов защиты; защита от отладок и дизассемблирования; способы встраивания защитных механизмов в программное обеспечение; понятие разрушающего программного воздействия; модели взаимодействия прикладной программы и программной закладки; методы перехвата и навязывания информации; методы внедрения программных закладок; компьютерные вирусы как особый класс разрушающих программных воздействий; защита от РПВ; понятие изолированной программной среды.

8. Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии. Возможности СИИТ для обеспечения комплексной защиты программ в момент их выполнения и данных при их обработке в компьютере; метод верификации программного обеспечения для контроля корректности, реализуемости и защиты от закладок.

9. Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов.

10. Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации; защита арифметических вычислений в компьютерных системах; основные направления создания защищенных компьютерных систем нового поколения на основе СИИТ.

## 2. Вопросы для подготовки к сдаче кандидатского экзамена с учетом отрасли науки

Экзаменационные вопросы к разделу 1:

1. Информация как объект правоотношений.

2. Понятие информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности.

3. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в Российской Федерации.

4. Понятие и виды защищаемой информации по законодательству РФ.

5. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.

6. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания.

7. Органы защиты государственной тайны и их компетенция.

8. Организационные меры, направленные на защиту государственной тайны. Порядок допуска и доступа к государственной тайне.

9. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).

10. Основные виды информации ограниченного доступа: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна, тайна следствия и судопроизводства.

11. Правовые режимы информации ограниченного доступа: содержание и особенности.

12. Основные требования, предъявляемые к организации защиты информации ограниченного доступа.

13. Юридическая ответственность за нарушения правовых режимов информации ограниченного доступа (дисциплинарная, гражданско-правовая, административная и уголовная).

14. Понятия лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию.

15. Объекты лицензирования. Органы лицензирования и их полномочия. Контроль за соблюдением лицензиатами условий ведения деятельности.

16. Понятие сертификации по российскому законодательству. Правовая регламентация сертификационной деятельности в области обеспечения информационной безопасности.

17. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия.

18. Понятие и виды интеллектуальных прав.

19. Объекты и субъекты авторского права. Авторские права (личные неимущественные права и исключительное право).

20. Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав. Ответственность за разглашение информации, отнесенной к государственной тайне.

21. Организация служебного расследования по фактам разглашения и утечки конфиденциальной информации.

22. Подбор сотрудников на должности, связанные с работой с конфиденциальной информацией, и текущая работа с ними.

23. Понятие организационной защиты информации. Место ОЗИ в системе информационной безопасности предприятия.

24. Организация охраны территории, зданий, помещений и сотрудников. Организация пропускного и внутриобъектового режимов.

25. Допуск и доступ к государственной, служебной тайнам и персональным данным сотрудников.

26. Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия.

27. Классификация носителей защищаемой информации.

28. Защита информации в центрах обработки данных.

29. Каналы и методы несанкционированного доступа к информации.

30. Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к информации.

Экзаменационные вопросы к разделу 2:

1. Традиционные симметричные криптосистемы. Основные понятия и определения.

2. Шифры перестановки, шифры простой замены.

3. Методы шифрования (полибианский квадрат; система шифрования Цезаря; система шифрования Вижинера; шифр «двойной квадрат» Уитстона; одноразовая система шифрования; шифрование методом Вернама).

4. Роторные машины; шифрование методом гаммирования; методы генерации псевдослучайных последовательностей чисел.

5. Применение симметричных криптосистем для защиты компьютерной информации в информационных системах.

Американский стандарт шифрования данных DES.

6. Отечественный стандарт шифрования данных.

7. Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах.

8. Концепция криптосистемы с открытым ключом. .

9. Безопасность и быстродействие криптосистемы RSA; комбинированный метод шифрования.

10. Методы идентификации и проверки подлинности пользователей компьютерных систем. Основные понятия и концепции.

11. Идентификация и механизмы подтверждения подлинности пользователя; протоколы и упрощенная схема идентификации с нулевой передачей знаний.

12. Проблема аутентификации данных и электронная цифровая подпись.

13. Однонаправленные хэш-функции.

14. Алгоритмы цифровой подписи RSA.

15. Защита компьютерных систем от удаленных атак через сеть Internet. Режим функционирования межсетевых экранов и их основные компоненты.

16. Маршрутизаторы; шлюзы сетевого уровня; усиленная аутентификация.

17. Основные схемы сетевой защиты на базе межсетевых экранов; применение межсетевых экранов для организации виртуальных корпоративных сетей.

18. Программные методы защиты от удаленных атак.

19. Существующие аппаратно-программные средства криптографической защиты компьютерной информации серии КРИПТОН.

20. Основные элементы средств защиты сети от несанкционированного доступа.

21. Абонентское шифрование и ЭЦП; шифрование пакетов; аутентификация; защита компонентов ЛВС от НСД.

22. Защита абонентского пункта, маршрутизаторов и устройств контроля; технология работы с ключами.

23. Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов).

24. Классификация способов защиты.

25. Разрушающее программное воздействие; модели взаимодействия прикладной программы и программной закладки; методы перехвата и навязывания информации; методы внедрения программных закладок.

26. Компьютерные вирусы как особый класс разрушающих программных воздействий; защита от РПВ; понятие изолированной программной среды.

27. Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.

28. Возможности СИИТ для обеспечения комплексной защиты программ в момент их выполнения и данных при их обработке в компьютере.

29. Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации.

30. Основные направления создания защищенных компьютерных систем нового поколения на основе СИИТ.

## 3. Перечень основной и дополнительной учебной литературы

### 3.1 Основная литература

1. Исаев, А. С. Правовые основы организации защиты персональных данных: учебное пособие / А. С. Исаев, Е. А. Хлюпина. — Санкт-Петербург : НИУ ИТМО, 2014. — 106 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/71004 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

2. Организационно-правовое обеспечение информационной безопасности: учебник / А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев [и др.] ; под редакцией А. А. Александрова, М. П. Сычева. — Москва : МГТУ им. Баумана, 2018. — 291 с. — ISBN 978-5-7038-4723-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/172840 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

3. Информационные технологии. Базовый курс : учебник для вузов / А. В. Костюк, С. А. Бобонец, А. В. Флегонтов, А. К. Черных. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 604 с. — ISBN 978-5-8114-8776-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180821 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

4. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

5. Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2. — Текст : электронный // Лань : электронно-библиотечная система. —

URL: https://e.lanbook.com/book/132242 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

6. Введение в теоретико-числовые методы криптографии : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург : Лань, 2021. — 400 с. — ISBN 978-5-8114-1116-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167921 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

7. Рябко, Б. Я. Основы современной криптографии и стеганографии : монография / Б. Я. Рябко, А. Н. Фионов. — 2-е изд. — Москва : Горячая линия-Телеком, 2016. — 232 с. — ISBN 978-5-9912-0350-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111098 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

8. Мошак, Н. Н. Защищенные информационные системы : учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180099 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

9. Чернокнижный, Г.М. Администрирование средств защиты информации в компьютерных системах и сетях: учебное пособие. — Санкт-Петербург, 2020. — 90 с. — URL: https://elibrary.ru/item.asp?id=46410288 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

10. Программно-аппаратные средства защиты информации : учебное пособие / Л. Х. Мифтахова, А. Р. Касимова, В. Н. Красильников [и др.]. — Санкт-Петербург : Интермедия, 2018. — 408 с. — ISBN 978-5-4383-0157-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103200 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

11. Зайцев, А. П. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111057 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

12. Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161337 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

13. Исаева, М. Ф. Техническая защита информации : учебное пособие / М. Ф. Исаева. — Санкт-Петербург : ПГУПС, 2017. — 49 с. — ISBN 978-5-7641-1008-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL:

https://e.lanbook.com/book/101600 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

### 3.2 Дополнительная литература

1. Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) : учебное пособие / В. К. Новиков. — Москва : Горячая линия-Телеком, 2017. — 176 с. — ISBN 978-5-9912-0525-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111084 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

2. Шилкина, М. Л. Защита информации и информационная безопасность: текст лекций : учебное пособие / М. Л. Шилкина. — Санкт-Петербург : СПбГЛТУ, 2011. — 144 с. — ISBN 978-5-9239-0413-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/45471 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

3. Голиков, А. М. Методы шифрования информации в сетях и системах радиосвязи : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2012. — 329 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/11380 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

4. Музыкантский, А. И. Лекции по криптографии : учебное пособие / А. И. Музыкантский, В. В. Фурин. — 2-е изд. — Москва : МЦНМО, 2013. — 68 с. — ISBN 978-5-4439-2075-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/56408 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

5. Программно-аппаратные средства защиты информации : учебно-методическое пособие / С. И. Штеренберг, А. М. Гельфанд, Д. В. Рыжаков, Р. А. Фатхутдинов. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. — 98 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180093 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

6. Костин, В. Н. Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации : учебное пособие / В. Н. Костин. — Москва : МИСИС, 2018. — 21 с. — ISBN 978-5-906953-22-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/116744 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

7. Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 2-е изд. — Москва : ИНТУИТ, 2016. — 424 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL:

https://e.lanbook.com/book/100275 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

8. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110328 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

9. Каторин, Ю. Ф. Техническая защита информации: Лабораторный практикум / Ю. Ф. Каторин, А. В. Разумовский, А. И. Спивак ; под редакцией Ю. Ф. Каторина. — Санкт-Петербург : НИУ ИТМО, 2013. — 112 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/71124 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

10. Сертификация средств защиты информации : учебное пособие / А. А. Миняев, Юркин, М. М. Ковцур, К. А. Ахрамееева. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 88 с. — ISBN 978-5-89160-213-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180100 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

11. Булычев, Г. Г. Программно-аппаратные средства обеспечения информационной безопасности : методические рекомендации / Г. Г. Булычев. — Москва : РТУ МИРЭА, 2020 — Часть 1 — 2020. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163932 (дата обращения: 24.02.2022). — Режим доступа: для авториз. пользователей.

## 4. Условия допуска к экзамену

К сдаче кандидатских экзаменов допускаются аспиранты, а также лица, имеющие высшее образование, подтвержденное дипломом специалиста или магистра, прикрепленные для подготовки диссертации на соискание ученой степени кандидата наук, сдачи кандидатских экзаменов без освоения программ подготовки научно-педагогических кадров в аспирантуре.

## 5. Процедура проведения экзамена

Прием кандидатского экзамена по специальной дисциплине проводится в виде письменного экзамена и последующего собеседования по представленным ответам в очной форме в аудитории университета.

Процедура проведения кандидатского экзамена по специальной дисциплине:

1. В аудиторию заходят все Соискатели, присутствующие на экзамене.

2. Председатель комиссии или его заместитель поочередно называет фамилию, имя и отчество Соискателя из числа присутствующих и просит экзаменуемого Соискателя предъявить документы, удостоверяющие личность Соискателя.

3. После подтверждения личности Соискателя, комиссия просит Соискателя назвать номер из числа оставшихся номеров вопросных листов (билетов). Вопросный лист содержит 3 экзаменационных вопроса из разных тем, представленных в программе кандидатского экзамена по специальной дисциплине. Председатель или член комиссии зачитывает экзаменационные вопросы, указанные в выбранном вопросном листе, озвучивает текущее время как время начала подготовки Соискателя к собеседованию. Фамилия, имя, отчество Соискателя, номер вопросного листа, и время начала подготовки фиксируются комиссией в ведомости кандидатского экзамена по специальной дисциплине. Соискатель начинает письменную подготовку к собеседованию по выбранному билету.

4. Время подготовки Соискателя к собеседованию – не менее 45 минут.

5. Соискатель имеет право заявить о своей готовности к собеседованию по заданным темам ранее отведенного ему времени.

6. По окончании отведенного времени Комиссия проводит собеседование с Соискателями в порядке выдачи вопросных листов, либо ранее, по желанию Соискателя.

7. Соискатель проходит устное индивидуальное собеседование на основе представленных письменных ответов на выданные вопросы. Количество дополнительных вопросов не более трех: по одному из каждой темы.

8. Комиссия оценивает ответы Соискателя и проставляет оценку в соответствующей ведомости.

9. После заслушивания ответов всех Соискателей комиссия оглашает результаты экзамена.

10. По результатам экзамена по каждому Соискателю оформляется протокол заседания экзаменационной комиссии по приему кандидатского экзамена.