ПРОГРАММА
вступительного экзамена по образовательной программе высшего образования – программе подготовки научных и научно-педагогических кадров в аспирантуре по научной специальности 2.3.6 Методы и системы защиты информации, информационная безопасность
(группа научных специальностей 2.3. Информационные технологии и телекоммуникации)

1. Организация вступительного испытания

Форма проведения вступительного испытания*:* устный ответ на вопросы экзаменационного билета. Билет вступительного испытания содержит 2 вопроса.

Язык проведения вступительных испытаний – русский.

2. Содержание вступительного экзамена.

№ п/п	Наименование раздела дисциплины	Содержание
	Раздел 1. Основы информационной безопасности	
1.	Тема 1. Теоретические основы ИБ	Модели систем дискреционного разграничения доступа. Модели систем мандатного разграничения доступа. Модели ролевого разграничения доступа. Модели безопасности информационных потоков. Принципы комплексного обеспечения ИБ. P.D.C.A.-циклы Деминга. Принципы Керкгоффса. Принципы криптографии и шифрования.
2.	Тема 2. Классификация и категорирование объектов защиты	Основные нормативно-правовые акты для различных видов объектов защиты. Уровни контроля на отсутствие недекларированных возможностей (НДВ). Классификация средств защиты. Категорирование защищаемой информации. Категорирование ИСПДн и требования по защите. Классификация АС и требования по защите. Классификация СВТ и требования по защите. Категорирование объектов КИИ и требования по защите
3.	Тема 3. Аттестация и аудит ИБ	Этапы и правила проведения аудита ИБ. Стандарты аудита ИБ. Процесс аттестации объекта информатизации. Стандарты аттестации объектов информатизации. Общие критерии оценки средств защиты информации. Реестр сертифицированных СЗИ. Реестр лицензий на криптографию.

Раздел 2. Средства защиты информации		
4.	Тема 4. Контроль доступа	Протокол AAA. Парольная защита. Токены. Биометрика и поведенческий анализ. Многофакторная аутентификация. Протоколы сетевой аутентификации. Средства доверенной загрузки. Файловые и сетевые ACL. Системы журналирования событий безопасности. Электронная подпись.
5.	Тема 5. Обеспечение сетевой безопасности	Анализ сетевого траффика. Блокирование нежелательного трафика. Сегментирование сетевой инфраструктуры. Системы обнаружения вторжений. VLAN. VPN. Proxy.
6.	Тема 6. Защита конечных точек	Инфраструктура безопасности Windows. Контроль доступа. Групповая политика безопасности. Управление ролями и службами ОС. Архитектура безопасности Linux. Разграничение доступа в Linux. Утилиты безопасности Linux. Управление конфигурацией и службами Linux. Антивирусная защита. Контроль действий пользователей, защита от утечек (DLP).
	Раздел 3. Система управления информационной безопасностью	
7.	Тема 7. Управление рисками информационной безопасности	Методологии риск-менеджмента. Методы анализа риска. Методики оценки риска. Способы обработки риска. Система управления ИБ. Политика безопасности. Жизненный цикл систем управления ИБ. ISO 27000
8.	Тема 8. Управление угрозами и уязвимостями ИБ	Базы данных общеизвестных уязвимостей ИБ. Количественная оценка уязвимостей. Классификация атак и техник. Сбор данных об угрозах (Thread Intelligence). Сканеры уязвимостей.
9.	Тема 9. Управление инцидентами	Процесс реагирования на инцидент и сценарии реагирования (плейбуки). Мониторинг компьютерных сетей, сетевого оборудования, конечных узлов. Унифицированный формат описания правил детектирования (Sigma Rules). SIEM. Extended Detection and Response (XDR). Принципы компьютерной форензики. Восстановление данных. Оперативные центры обеспечения кибербезопасности (Security Operations Center, SOC). Платформы реагирования на инциденты (Incident Response Platform, IRP)

3. Перечень вопросов к вступительному экзамену.

1. Приведите примеры моделей систем дискреционного разграничения доступа.
2. Приведите примеры моделей систем мандатного разграничения доступа.
3. Приведите примеры моделей ролевого разграничения доступа.
4. Приведите примеры моделей безопасности информационных потоков.
5. Приведите пример системы защиты и используемые в ней принципы ИБ.
6. Приведите пример ассиметричной системы шифрования.
7. Напишите основные нормативно-правовые акты для различных видов объектов защиты.
8. Опишите уровни контроля на отсутствие недекларированных возможностей (НДВ).
9. Сопоставьте классификацию средств защиты информацию и категорию защищаемой информации.
10. Какие существуют классы защищенности ИСПДн.
11. Опишите требования по защите различных классов АС.
12. Опишите требования по защите различных классов СВТ.
13. Опишите требования по защите различных категорий значимостей КИИ.
14. Приведите пример проведения аудита ИБ какой-либо информационной системы.
15. Приведите описание процесса аттестации объекта информатизации.
16. Общие критерии оценки средств защиты информации.
17. Опишите основные этапы включения в реестр сертифицированных СЗИ или порядок получения лицензий на криптографию.
18. Приведите пример системы аутентификации, авторизации и аудита действий пользователя.
19. Опишите способы оценки пароля на стойкость, надежность, набираемость, запоминаемость.
20. Опишите принцип работы токенизации.
21. Опишите методы оценки ошибок в биометрии и поведенческом анализе.
22. Приведите пример средства многофакторной аутентификации.
23. Приведите примеры протоколов сетевой аутентификации с оценкой надежности.
24. Опишите возможности средств доверенной загрузки.
25. Опишите возможности файловых и сетевых ACL.
26. Приведите примеры систем журналирования событий безопасности.
27. Опишите принципы использования квалифицированной электронной подписи.
28. Приведите примеры использования анализаторов сетевого траффика.
29. Опишите правила блокирования нежелательного трафика при подмене адреса.
30. Приведите примеры правил для сегментирования сетевой инфраструктуры.
31. Приведите пример систем обнаружения вторжений.
32. Опишите принцип работы и стандарты VLAN.
33. Опишите принцип работы и стандарты VPN.
34. Опишите принцип работы и виды Proxy.
35. Опишите принцип работы инфраструктуры безопасности Windows.
36. Опишите принципы контроля доступа и групповая политика безопасности Winodws.
37. Приведите примеры безопасного управления ролями и службами ОС.
38. Опишите принципы безопасности Linux.
39. Опишите принципы разграничения доступа в Linux.
40. Приведите примеры применения утилит безопасности Linux.
41. Опишите способы оценки эффективности антивирусной защиты.
42. Приведите пример системы защиты от утечек (DLP).
43. Опишите наиболее известные методологии риск-менеджмента.
44. Приведите пример анализа и оценки рисков.
45. Сопоставьте способы обработки риска и основные положения политики безопасности СУИБ.
46. Опишите основные этапы построения системы защиты по ISO 27000.

47. Приведите пример выявления и оценки уязвимости по исходному коду.
48. Приведите пример цепочки атаки (kill-chain).
49. Опишите способы сбора данных об угрозах (Thread Intelligence).
50. Опишите основные возможности существующих сканеров уязвимостей.
51. Опишите процесс реагирования на какой-либо инцидент.
52. Опишите принципы мониторинга компьютерных сетей, сетевого оборудования, конечных узлов.
53. Приведите пример использования Sigma Rules.
54. Опишите основные возможности существующих SIEM.
55. Опишите основные возможности существующих XDR-систем.
56. Опишите основные принципы компьютерной форензики.
57. Приведите примеры восстановление данных с различных носителей.
58. Опишите структуру и требования к оперативным центрам обеспечения кибербезопасности (Security Operations Center, SOC).
59. Опишите основные возможности существующих платформы реагирования на инциденты (Incident Response Platform, IRP).

4. Шкала оценивания, минимальное количество баллов, подтверждающее успешное прохождение вступительного испытания, максимальное количество баллов.

Уровень знаний поступающего оценивается экзаменационной комиссией по **100-балльной шкале**. Минимальное количество баллов, подтверждающее успешное прохождение вступительного испытания, составляет **50 (пятьдесят) баллов**. Максимальное количество баллов составляет **100 (сто) баллов**.

Шкала оценивания на вступительном испытании по специальной дисциплине:

4. Шкала оценивания, минимальное количество баллов, подтверждающее успешное прохождение вступительного испытания, максимальное количество баллов.

Уровень знаний поступающего оценивается экзаменационной комиссией по **100-балльной шкале**. Минимальное количество баллов, подтверждающее успешное прохождение вступительного испытания, составляет **50 (пятьдесят) баллов**. Максимальное количество баллов составляет **100 (сто) баллов**.

Шкала оценивания на вступительном испытании по специальной дисциплине:

Оценка *«100 – 76» – «5» баллов (по пятибалльной шкале) выставляется, если поступающий демонстрирует:*

- глубокие знания основных понятий в области научной специальности, умение оперировать ими;
- высокую степень полноты и точности рассмотрения основных вопросов, раскрытия темы;
- отличное умение представить основные вопросы в научном контексте;
- отличное владение научным стилем речи.

Оценка «75 – 64» – «4» балла (по пятибалльной шкале) выставляется, если поступающий демонстрирует:

- хорошие знания основных положений в области научной специальности, умение оперировать ими, демонстрируются единичные неточности;
- достаточная степень полноты и точности рассмотрения основных вопросов, раскрытия темы, демонстрируются единичные неточности;
- единичные (негрубые) стилистические и речевые погрешности;
- умение защитить ответы на основные вопросы;
- хорошее владение научным стилем речи.

<u>Оценка «63 – 50» – «3» балла (по пятибалльной шкале)</u> выставляется, если поступающий демонстрирует:

- удовлетворительные знания основных понятий в области научной специальности, умение оперировать ими, неточности знаний;
- удовлетворительная степень полноты и точности рассмотрения основных вопросов, раскрытия темы;
- посредственные ответы на вопросы.

<u>Оценка «менее 50» – «2» балла (по пятибалльной шкале</u>) выставляется, если поступающий демонстрирует:

- грубые ошибки в знании основных положений в области научной специальности;
- отсутствие знаний основных положений в области научной специальности, умения оперировать ими;
- недостаточное владение научным стилем речи;
- не умение защитить ответы на основные вопросы.

5. Рекомендуемая литература

Рекомендуемая основная литература

№	Название
1.	Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode.
2.	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2023. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511239.
3.	Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998.
4.	Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2023. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511138.
5.	Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2023. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511890.
6.	Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/513300.

Рекомендуемая дополнительная литература

№	Название
1.	Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268.
2.	Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927.
3.	Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2023. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511700.
4.	Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2023. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512423.
5.	Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/515435.
6.	Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов / Н. С. Козырь, Н. В. Седых. — Москва : Издательство Юрайт, 2023. — 170 с. — (Высшее образование). — ISBN 978-5-534-17153-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/532474.

Программное обеспечение и Интернет-ресурсы.

(Включает в себя перечень электронных учебников, учебных пособий, наборы презентаций, программное обеспечение, Интернет-ресурсов (название и web-адрес) и пр.)

1. Справочная правовая система: "КонсультантПлюс" - законодательство РФ: кодексы, законы, указы, постановления Правительства Российской Федерации, нормативные акты (consultant.ru)

2. Справочная правовая система: ГАРАНТ - Законодательство (кодексы, законы, указы, постановления) РФ, аналитика, комментарии, практика. (garant.ru)

3. Главная - ФСТЭК России (fstec.ru)