Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Алтайский государственный университет»

ПРОГРАММА
вступительного испытания для поступающих в магистратуру ИЦТЭФ 2024г.

Направление подготовки
10.04.01 Информационная безопасность

профиль «Информационная безопасность интеллектуальных автоматизированных систем»

Экзамен по направлению «Информационная безопасность»
(письменно)

2024

I. Вводные замечания (по форме проведения вступительных испытаний)

1. Форма проведения экзамена – письменно. Продолжительность экзамена – 3 астрономических часа. Каждый экзаменационный билет содержит четыре вопроса. В качестве вопросов формулируются основные положения из предметной области, предполагающее их развернутое обоснование при ответе.

2. Критерий оценки. Каждый вопрос оценивается от 0 до 25 баллов. Итоговая экзаменационная оценка формируется по сумме баллов. Минимальное количество баллов, дающее право участвовать в конкурсе на поступление в магистратуру - 30.

II. Программа вступительных испытаний

Основные понятия защиты информации (субъекты, объекты, доступ, информационные потоки). Постановка задачи построения защищенной автоматизированной системы.

Угрозы безопасности информации. Угрозы конфиденциальности, целостности, доступности, раскрытия параметров автоматизированной системы.

Понятие политики безопасности. Дискреционная политика безопасности. Мандатная политика безопасности. Мандатная политика целостности.

Модель Белла-Лападулы как основа построения систем мандатного разграничения доступа. Основные положения модели. Базовая теорема безопасности.

Основные положения критериев TCSEC. Фундаментальные требования компьютерной безопасности. Требования классов защиты.

Основные положения руководящих документов ГТК в области защиты информации. Определение и классификация НСД. Определение и классификация нарушителя.

Классы защищенности автоматизированных систем от несанкционированного доступа к информации.

Классификация сетей по способам распределения данных. Сравнительная характеристика различных типов сетей.

Основы организации и функционирования сетей.

Общая характеристика операционных систем. Назначение и возможности систем семейств UNIX и Windows.

Основные механизмы безопасности: средства и методы аутентификации в операционных системах. Модели разграничения доступа.

Организация и использование средств аудита.

Администрирование операционных систем: основные задачи и принципы сопровождения системного программного обеспечения. Управления безопасностью операционных систем.

Основные сетевые стандарты: средства взаимодействия процессов в сетях, распределенная обработка информации в системах клиент-сервер.

Безопасность ресурсов сети: средства идентификации и аутентификации.

Методы разделения ресурсов и технологии разграничения доступа.

Основные принципы построения локальных вычислительных сетей. Особенности организации сетей на базе ОС NetWare, Windows, UNIX.

Организация проектирования комплексной системы обеспечения информационной безопасности автоматизированной системы (нормативные документы, этапность, содержание работ).

Виды, источники и носители защищаемой информации. Структура, классификация и основные характеристики технических каналов утечки информации

Побочные электромагнитные излучения и наводки.

Концепция, методы и средства инженерно-технической защиты информации.

Скрытие акустических информативных сигналов.

Обнаружение и локализация закладных устройств, подавление их сигналов.

Принципы создания программно-аппаратных средств обеспечения информационной безопасности.

Концепция диспетчера доступа. Методы и средства ограничения доступа к компонентам вычислительных систем.

Способы встраивания средств защиты в программное обеспечение.

Защита от разрушающих программных воздействий. Защита программ от изменения и контроль целостности.

Программно-аппаратные средства защиты информации в сетях и системах передачи данных.

Примерные вопросы к экзамену

1. Принципы построения защищенной автоматизированной системы.
2. Угрозы безопасности информации.
3. Мандатная политика безопасности.
4. Основные положения модели Белла-Лападулы.
5. Фундаментальные требования компьютерной безопасности.
6. Основные положения руководящих документов ГТК в области защиты информации.
7. Классы защищенности автоматизированных систем от несанкционированного доступа к информации.
8. Классификация сетей по способам распределения данных.
9. Основы организации и функционирования сетей.
10. Общая характеристика операционных систем.
11. Средства и методы аутентификации в операционных системах.
12. Организация и использование средств аудита.

13. Управления безопасностью операционных систем.
14. Основные сетевые стандарты.
15. Средства идентификации и аутентификации.
16. Методы разделения ресурсов и технологии разграничения доступа.
17. Особенности организации сетей на базе ОС NetWare, Windows, UNIX.
18. Организация проектирования комплексной системы обеспечения информационной безопасности автоматизированной системы.
19. Основные характеристики технических каналов утечки информации
20. Побочные электромагнитные излучения и наводки.
21. Методы и средства инженерно-технической защиты информации.
22. Скрытие акустических информативных сигналов.
23. Обнаружение и локализация закладных устройств.
24. Методы и средства ограничения доступа к компонентам вычислительных систем.
25. Способы встраивания средств защиты в программное обеспечение.
26. Защита программ от изменения и контроль целостности.
27. Программно-аппаратные средства защиты информации в сетях и системах передачи данных.

III. Список учебно-методической литературы, достаточный для подготовки к вступительным испытаниям (в том числе для абитуриентов, поступающих не по профилю полученного ранее образования)

1. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. – М.: Изд-во «Машиностроение», 2007.
2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: - 2-е изд., стер.- М.: Изд-во «Академия», 2006.
3. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации: учеб.пособие для вузов. - 2-е изд., стер.- М.: Изд-во «Академия», 2007.
4. Девянин П.Н. Модели безопасности компьютерных систем.- М.: Изд-во «Академия», 2005.
5. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации.- М.: Горячая линия - Телеком, 2004.
6. Венбо Мао. Современная криптография. Теория и практика. М.: Вильямс, 2005.
7. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М.: Горячая линия - Телеком, 2005.
8. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. М.: Горячая линия Телеком, 2005.

9. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации. М.: Гелиос-АВ, 2005.
10. Прохода А.Н. Обеспечение Интернет-безопасности. М.: Горячая линия Телеком, 2007.