МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ЛИПЕЦКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Председатель приемной комиссии ЛГПУ
_____ Н.В. Федина
«24» марта 2016г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА ПО СПЕЦИАЛЬНОЙ ДИСЦИПЛИНЕ

НАПРАВЛЕНИЕ ПОДГОТОВКИ

10.06.01 - ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

НАПРАВЛЕННОСТЬ

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Липецк 2016

Данная программа включает вопросы экзамена при поступлении в аспирантуру Липецкого государственного педагогического университета по направлению подготовки 10.06.01 – Информационная безопасность, направленность – методы и системы защиты информации, информационная безопасность.

1. СОДЕРЖАНИЕ ПРОГРАММЫ

I. Теория информационной безопасности

Сущность и понятие информационной безопасности.

Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Структура информационной безопасности. Определение понятия "информационная безопасность".

Современная доктрина информационной безопасности Российской Федерации.

Понятие и назначение доктрины информационной безопасности.

Интересы личности, общества и государства в информационной сфере.

Виды и состав угроз информационной безопасности.

Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.

Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации.

Организационная основа системы обеспечения информационной безопасности.

Понятие уязвимости информации. Формы проявления уязвимости информации. Виды уязвимости информации. Понятие "утечка информации". Соотношение форм и видов уязвимости информации. Содержательная часть понятия "защита информации".

Критерии, условия и принципы отнесения информации к защищаемой.

Состав и классификация носителей защищаемой информации.

Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.

Обладатель информации. Обладатели информации, составляющей государственную тайну. Обладатели информации, составляющей коммерческую тайну. Обладатели информации, отнесенной к служебной и профессиональной тайне.

Понятие объекта защиты информации.

Носители информации как конечные объекты защиты. Особенности отдельных видов носителей как объектов защиты.

2. Правовая защита информации

Назначение и структура правового обеспечения защиты информации. Методы правовой защиты информации. Правовые основы защиты государственной, коммерческой, служебной, профессиональной и личной тайны, персональных данных. Система правовой ответственности за утечку

информации и утрату носителей информации. Понятие интеллектуальной собственности, ее виды и основные объекты образования. Интеллектуальный продукт как объект интеллектуальной собственности и предмет защиты. Содержание гражданско-правовых норм в области защиты интеллектуальной собственности. Авторское право; патентное право; товарный знак; договорное право, авторские и лицензионные договоры.

3. Физические основы защиты информации.

Поля объектов и проблемы защиты информации, физические поля различной природы как носители информации об объектах, общие принципы регистрации информативных характеристик полей. Электрические, магнитные и электромагнитные поля объектов, электромагнитные волны, их характеристики, свойства и особенности распространения, ближняя и дальняя зоны излучателя, распространение полей в неоднородных средах, принципы экранирования статических и динамических полей. Упругие волны, их характеристики, основы акустики речи и слуха, специфика акустики помещений, звукоизоляция, инфразвук, ультразвук.

4. Инженерно-техническая защита информации.

Виды информации, защищаемой техническими средствами. Демаскирующие признаки объектов защиты. Источники и носители информации, защищаемой техническими средствами. Принципы записи и съема информации с носителей. Виды угроз безопасности информации, защищаемой техническими средствами. Принципы добывания и обработки информации техническими средствами. Классификация и структура технических каналов утечки информации. Основные способы и принципы работы средств наблюдения объектов, подслушивания и перехвата сигналов. Способы и принципы работы средств защиты информации от наблюдения, подслушивания и перехвата.

Организационные и технические меры инженерно-технической защиты информации в государственных и коммерческих структурах.

Роль и место технических средств в организации режима охраны, современная концепция защиты объектов. Основные составляющие систем ТСО: датчики, приборы визуального наблюдения, системы сбора и обработки информации, средства связи, питания и тревожно-вызывной сигнализации.

5. Криптографическая защита информации.

Классические шифры, шифры гаммирования и колонной замены. Простейшие шифры и их свойства. Композиции шифров. Системы шифрования с открытыми ключами. Криптографическая стойкость шифров. Основные требования к шифрам. Имитостойкость и помехоустойчивость шифров. Принципы построения криптографических алгоритмов. различие между программными и аппаратными реализациями. Криптографические параметры узлов и блоков шифраторов. Методы получения случайных и псевдослучайных последовательностей. Программные реализации шифров. Особенности использования вычислительной техники в криптографии. Вопросы организации

сетей засекреченной связи. Ключевые системы, криптографические хеш-функции. Электронная цифровая подпись. Криптографические протоколы.

2. Вопросы к вступительному экзамену в аспирантуру

1. Сущность и понятие информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Структура информационной безопасности. Определение понятия "информационная безопасность".
2. Основные способы и принципы работы средств наблюдения объектов, подслушивания и перехвата сигналов. Способы и принципы работы средств защиты информации от наблюдения, подслушивания и перехвата.
3. Современная доктрина информационной безопасности Российской Федерации. Понятие и назначение доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере.
4. Роль и место технических средств в организации режима охраны, современная концепция защиты объектов. Основные составляющие систем ТСО: датчики, приборы визуального наблюдения, системы сбора и обработки информации, средства связи, питания и тревожно-вызывной сигнализации.
5. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации. Организационная основа системы обеспечения информационной безопасности.
6. Классические шифры, шифры гаммирования и колонной замены. Простейшие шифры и их свойства. Композиции шифров. Криптографическая стойкость шифров. Основные требования к шифрам. Имитостойкость и помехоустойчивость шифров.
7. Понятие уязвимости информации. Формы проявления уязвимости информации. Виды уязвимости информации. Понятие "утечка информации". Соотношение форм и видов уязвимости информации. Содержательная часть понятия "защита информации".
8. Системы шифрования с открытыми ключами. Принципы построения криптографических алгоритмов. Различие между программными и аппаратными реализациями. Криптографические параметры узлов и блоков шифраторов.
9. Обладатель информации. Обладатели информации, составляющей государственную тайну. Обладатели информации, составляющей коммерческую тайну. Обладатели информации, отнесенной к служебной и профессиональной тайне.
10. Упругие волны, их характеристики, основы акустики речи и слуха, специфика акустики помещений, звукоизоляция, инфразвук, ультразвук.
11. Назначение и структура правового обеспечения защиты информации. Методы правовой защиты информации.
12. Электрические, магнитные и электромагнитные поля объектов, электромагнитные волны, их характеристики, свойства и особенности

распространения, ближняя и дальняя зоны излучателя, распространение полей в неоднородных средах, принципы экранирования статических и динамических полей.

13. Правовые основы защиты коммерческой, служебной, профессиональной и личной тайны. Система правовой ответственности за утечку информации и утрату носителей информации.
14. Криптографические протоколы. Вопросы организации сетей засекреченной связи.
15. Виды и состав угроз информационной безопасности. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.
16. Методы получения случайных и псевдослучайных последовательностей. Программные реализации шифров. Особенности использования вычислительной техники в криптографии.
17. Авторское право; патентное право; товарный знак; договорное право, авторские и лицензионные договоры.
18. Поля объектов и проблемы защиты информации, физические поля различной природы как носители информации об объектах, общие принципы регистрации информативных характеристик полей.
19. Критерии, условия и принципы отнесения информации к защищаемой. Состав и классификация носителей защищаемой информации. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.
20. Принципы добывания и обработки информации техническими средствами. Классификация и структура технических каналов утечки информации.
21. Понятие интеллектуальной собственности, ее виды и основные объекты образования. Интеллектуальный продукт как объект интеллектуальной собственности и предмет защиты. Содержание гражданско-правовых норм в области защиты интеллектуальной собственности.
22. Принципы записи и съема информации с носителей. Виды угроз безопасности информации, защищаемой техническими средствами.
23. Понятие объекта защиты информации. Носители информации как конечные объекты защиты. Особенности отдельных видов носителей как объектов защиты.
24. Ключевые системы, криптографические хеш-функции. Электронная цифровая подпись.
25. Правовые основы защиты государственной тайны.
26. Организационные и технические меры инженерно-технической защиты информации в государственных и коммерческих структурах.
27. Правовые основы защиты персональных данных.
28. Виды информации, защищаемой техническими средствами. Демаскирующие признаки объектов защиты. Источники и носители информации, защищаемой техническими средствами.

Литература

1. Буйневич М.В., Доценко С.М., Малыш В.Н. Информационная безопасность и защита информации в компьютерных системах. Учебное пособие. – Липецк.: ЛГПУ, 2007. – 255 с.

2. Ярочкин В.И. Информационная безопасность. Учебник для вузов. – М.: Академический мир, 2002. – 640 с.

3. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие. – М.: Горячая линия - Телеком, 2004. – 280 с.

4. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2005. – 960 с.

5. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие. – М.: Горячая линия - Телеком, 2006. – 544 с.