МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

по направлению подготовки
10.04.01 Информационная безопасность
Направленность (профиль): «Комплексная защита инфокоммуникационных объектов»
Квалификация:
Магистр

Пятигорск, 2020

Содержание

1. Пояснительная записка

Вступительные испытания по направлению подготовки 10.04.01 «Информационная безопасность» направленность (профиль): «Комплексная защита инфокоммуникационных объектов» (очная форма обучения) проводятся для лиц, желающих освоить программу специализированной подготовки магистра по данному направлению.

Цель вступительных испытаний заключается в определении способностей совершенствования и развития своего интеллектуального и общекультурного уровня к самостоятельному обучению и приобретению новых знаний, а также профессиональных компетенций в способности проектировать сложные системы и комплексы защиты инфокоммуникационных объектов лиц, поступающих в магистратуру.

Лица, желающие освоить программу специализированной подготовки магистра, должны иметь высшее профессиональное образование определенной ступени, подтвержденное документом государственного образца, независимо от специальности и направления подготовки и успешно прошедшие вступительные испытания.

Магистр по направлению подготовки **10.04.01 Информационная безопасность** должен быть подготовлен к решению профессиональных задач в соответствии с профильной направленностью магистерской программы и видами профессиональной деятельности:

проектная деятельность:

– системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности;

– обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

– разработка систем, комплексов, средств и технологий обеспечения информационной безопасности;

– разработка программ и методик, испытаний средств и систем обеспечения информационной безопасности;

научно-исследовательская деятельность:

– анализ фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества;

– разработка планов и программ проведения научных исследований и технических разработок, подготовка отдельных заданий для исполнителей;

– выполнение научных исследований с применением соответствующих физических и математических методов;

– подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях;

контрольно-аналитическая деятельность:

– аудит информационной безопасности информационных систем и объектов информатизации;

– аттестация объектов информатизации по требованиям безопасности информации;

педагогическая деятельность:

– выполнение учебной (преподавательской) и методической работы в организациях, осуществляющих образовательную деятельность, по дисциплинам (модулям) соответствующих профилю подготовки;

организационно-управленческая деятельность:

– организация работы коллектива исполнителей, принятие управленческих решений, определение порядка выполнения работ;

– организация управления информационной безопасностью;

– организация работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации (далее - ФСБ России), Федеральной службы по техническому и экспортному контролю Российской Федерации (далее - ФСТЭК России);

– организация и выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

– разработка проектов организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

Программа по направлению подготовки 10.04.01 «Информационная безопасность» направленность (профиль): «Комплексная защита инфокоммуникационных объектов» предусматривает расширение сферы компетенции в области:

– защищенных информационных ресурсов и информационных технологий, компьютерных, автоматизированных, телекоммуникационных, информационных и информационно-аналитических системах.

– технологий обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта).

– методов и средств проектирования, моделирования и экспериментальной обработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации.

2. Содержание программы

1. Теория и методы комплексной защиты инфокоммуникационных объектов

1.1 Теория информационной безопасности

Сущность и понятие информационной безопасности, характеристика ее составляющих; значение информационной безопасности для субъектов информационных отношений; место информационной безопасности в системе национальной безопасности; современная концепция информационной безопасности; понятие и сущность защиты информации, ее место в системе информационной безопасности; цели и концептуальные основы защиты информации; критерии, условия и принципы отнесения информации к защищаемой; носители защищаемой информации; классификация конфиденциальной информации по видам тайны и степеням конфиденциальности; понятие и структура угроз защищаемой информации; источники, виды и методы дестабилизирующего воздействия на защищаемую информацию; причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию; виды уязвимости информации и формы ее проявления; каналы и методы несанкционированного доступа к конфиденциальной информации; направления, виды и особенности деятельности спецслужб по несанкционированному доступу к конфиденциальной информации; методологические подходы к защите информации и принципы ее организации; объекты защиты; виды защиты; классификация методов и средств защиты информации; кадровое и ресурсное обеспечение защиты информации; системы защиты информации.

1.2 Программно-аппаратная защита информации

Предмет и задачи программно-аппаратной защиты информации; идентификация субъекта, понятие протокола идентификации, идентифицирующая информация; основные подходы к защите данных от НСД; шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам; доступ к данным со стороны процесса; способы фиксации факта доступа; надежность систем ограничения доступа; защита файлов от изменения; электронная цифровая подпись (ЭЦП); программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных; защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты; методы и средства ограничения доступа к компонентам ЭВМ; защиты программ от несанкционированного копирования; пароли и ключи, организация хранения ключей; защита программ от излучения; защита от отладки, защита от дизассемблирования, защита от трассировки по прерываниям; защита от разрушающих программных воздействий (РПВ); компьютерные вирусы как особый класс РПВ; необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды.

1.3 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; системный подход к инженерно-технической защите информации; основные этапы проектирования системы защиты информации техническими средствами; принципы моделирования объектов защиты и технических каналов утечки информации; способы оценки угроз безопасности

информации и расходов на техническую защиту; 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; контроль эффективности защиты информации.

1.4 Методы проектирования систем технической охраны объектов

Автоматизированные, информационные технологии управления комплексными системами безопасности и жизнеобеспечения. Анализ угроз при проектировании автоматизированной комплексной системы безопасности. Основные требования при проектировании автоматизированной комплексной системы безопасности. Общие вопросы проектирования систем безопасности объектов. Стадии и этапы проектирования. Нормативная документация в области обеспечения безопасности. Нормативная документация по оформлению проектной документации. Принципы и правила оформления проектной документации. Проектирование объектов аппаратных и пультовых для систем безопасности.

3. Рекомендуемая литература (основная и дополнительная)

Основная литература:

1. Бабаш А.В. Информационная безопасность. Лабораторный практикум: учеб. пос. /А.В. Бабаш, Е.К. Баранова, Ю.Н.Мельников. – М.: КноРус, 2012

2. Васильков А.В. Безопасность и управление доступом в информационных системах: учеб. пос. / А.В.Васильков, И.А.Васильков. – М.: Форум, 2010

3. Гошко С.В. Технологии борьбы с компьютерными вирусами: практ. Пос. / С.В.Гошко. – М.: СолонПресс, 2009

4. Гошко С.В. Энциклопедия по защите от вирусов /С.В.Гошко. – М.:СОЛОН-Пресс, 2010

5. Информационная безопасность и защита информации: учеб. пос../Ю.Ю.Громов и др. – Старый Оскол: ТНТ, 2010

6. Ищейнов, В.Я. Защита конфиденциальной информации: учеб. пособие/ В. Я. Ищейнов, М. В. Мецатунян- М.: ФОРУМ, 2009.

7. Корнеев, И.К. Защита информации в офисе: учебник/ И. К. Корнеев, Е. А. Степанов- М.: ТК Велби, 2010

Дополнительная литература

1. Мельников В.П. Информационная безопасность и защита информации: учеб. пос. / В.П. Мельников, С.А.Клейменов, А.М. Петраков. – М.: Академия, 2011

2. Молдовян, Н.А. Практикум по криптосистемам с открытым ключом/ Н.А. Молдовян. – СПб.: БХВ-Петербург, 2007

3. Скляров О.К. Волоконно-оптические сети и системы связи: учеб. пос. /О.К.Скляров. – М.: Лань, 2010

4. Чипига А.Ф. Информационная безопасность автоматизированных систем: учеб. пос. / А.Ф. Чипига. – М.: Гелиос АРВ, 2010

5. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах / В.Ф.Шаньгин. – М.: Инфра-М, 2010

6. Фороузан, Б.А.Криптография и безопасность сетей: учеб. пособие / Б.А. Фороузан. – М.:.БИНОМ, 2010

7. Фостер, Д. Создание защищенных от вторжения прикладных программ: Д. Фостер; пер. с англ. А. А. Слинкин- М.: ДМК Пресс, 2009.

8. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие/ П. Б. Хорев- М.: ФОРУМ, 2009.

9. Технические средства и методы защиты информации: учеб. пособие/ А. П. Зайцев [и др.] ; ред.: А. П. Зайцев, А. А. Шелупанов- М.: Горячая линия - Телеком, 2009.

10. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие/ А. Ф. Чипига- М.: Гелиос АРВ, 2010.

11. Сергеева, Ю.С. Защита информации: конспект лекций/ Ю. С. Сергеева ; ред. А. В. Якушев- М.: ПРИОР, 2011.

12. Информационная безопасность и защита информации: учебное пособие/ Ю. Ю. Громов [и др.]- Старый Оскол: ТНТ, 2010.

13. ГОСТ Р 50 776-95 (МЭК 839-1-4-88) Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию.

14. Комплекс "Соболь". Руководство по администрированию УВАЛ. 00300-58 91

15. Комплекс "Соболь". Руководство пользователя УВАЛ. 00300-58 92

16. Secret Net 5.0-С. Сетевой вариант. Аппаратные средства УВАЛ. 00300-84 93

17. Secret Net 5.0-С. Сетевой вариант. Установка, обновление и удаление системы УВАЛ. 00300-84 92

18. Secret Net 5.0-C. Сетевой вариант. Руководство пользователя УВАЛ. 00300-84 96
19. Secret Net 5.0-C. Сетевой вариант. Управление системой УВАЛ. 00300-84 94
20. Secret Net 5.0-C. Сетевой вариант. Мониторинг, оперативное управление, аудит УВАЛ. 00300-84 95
21. Secret Net 5.0-C. Сетевой вариант. Принципы построения и применения УВАЛ. 00300-84 91