МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

КЫРГЫЗСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СТРОИТЕЛЬСТВА, ТРАНСПОРТА И АРХИТЕКТУРЫ ИМЕНИ Н. ИСАНОВА

Кафедра «Обеспечение безопасности информационных систем»

«УТВЕРЖДАЮ»
Ректор КГУСТА, д.т.н., профессор
_____ А.А. Абдыкалыков
«11» марта 2019 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ В МАГИСТРАТУРУ ПО СПЕЦИАЛЬНОЙ ДИСЦИПЛИНЕ

Направление подготовки: 590100 «Информационная безопасность»

Магистерская программа: Аудит информационной безопасности автоматизированных систем

Бишкек 2019

1. ОСНОВНЫЕ ПОЛОЖЕНИЯ

Настоящая программа описывает цели, содержание, форму, процедуру, критерии оценки и основную литературу, которая рекомендуется кафедрой «Обеспечение безопасности информационных систем» при подготовке к вступительному испытанию в магистратуру по направлению подготовки 590100 – Информационная безопасность.

Программа вступительного испытания в магистратуру по направлению 590100 «Информационная безопасность» составлена на основании Государственного образовательного стандарта высшего профессионального образования Кыргызской Республики подготовки бакалавра по направлению 590100 «Информационная безопасность» и охватывает базовые дисциплины подготовки бакалавров по названному направлению.

2. ЦЕЛЬ И ЗАДАЧИ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Цель вступительного испытания заключается в определении у поступающих базового уровня подготовки в предметной области, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере, необходимого для обучения в магистратуре по направлению подготовки 590100 – Информационная безопасность.

Задачи вступительного экзамена:

а) проверить у поступающих уровень ***знаний***:

- аппаратных средств вычислительной техники, операционных систем персональных ЭВМ;
- основ администрирования вычислительных сетей, систем управления базами данных;
- основных нормативных правовых актов в области информационной безопасности и защиты информации, а также нормативных методических документов министерств и ведомств Кыргызской Республики в данной области;
- правовых основ организации защиты государственной тайны и конфиденциальной информации, задач органов защиты государственной тайны;
- правовых норм и стандартов по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;
- принципов и методов организационной защиты информации;
- технических каналов утечки информации, возможностей технических разведок, способов и средств защиты информации от утечки по техническим каналам, методов и средств контроля эффективности технической защиты информации;
- принципов и методов противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;

- принципов организации информационных систем в соответствии с требованиями по защите информации;
- эталонной модели взаимодействия открытых систем, методов коммутации и маршрутизации, сетевых протоколов;

б) выявить уровень сформированности у поступающих ***умений***:

- формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;
- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- анализировать и оценивать угрозы информационной безопасности объекта;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- пользоваться нормативными документами по защите информации;
- применять на практике методы анализа электрических цепей;

в) выявить уровень ***владения*** поступающими:

- методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений;
- навыками выявления и уничтожения компьютерных вирусов;
- навыками работы с нормативными правовыми актами;
- методами и средствами выявления угроз безопасности автоматизированным системам;
- навыками организации и обеспечения режима секретности;
- методами технической защиты информации;
- методами формирования требований по защите информации;
- методами расчета и инструментального контроля показателей технической защиты информации;
- методами анализа и формализации информационных процессов объекта и связей между ними;
- методами организации и управления деятельностью служб защиты информации на предприятии;
- методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- профессиональной терминологией.

3. ОСНОВНЫЕ ТРЕБОВАНИЯ К ОТВЕТАМ ЭКЗАМЕНУЮЩЕГОСЯ

- имеет представление об установке, настройке, эксплуатации и поддержании в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

– понимает цели и задачи обеспечения защищенности объектов информатизации в условиях существования угроз в информационной сфере;
– оперирует предметной и методической терминологией;
– понимает основные положения нормативных правовых актов в области информационной безопасности и защиты информации;
– подтверждает основные положения теории практическими примерами;
– знает основные виды и способы защиты информации, угрозы безопасности информации, способы оценки соответствия требованиям по защите информации и эффективности защиты информации;
– умеет осуществлять администрирование подсистем информационной безопасности объекта информатизации, осуществлять организационно-правового обеспечения информационной безопасности объекта защиты;
– осведомлен о современных достижениях в области информационной безопасности;
– владеет навыками проведение проектных расчетов элементов систем обеспечения информационной безопасности;
– имеет опыт совершенствования системы управления информационной безопасностью;
– проявляет заинтересованность к проблемам информационной безопасности;
– имеет собственные оценочные суждения по вопросам обеспечения информационной безопасности.

4. СОДЕРЖАНИЕ ПРОГРАММЫ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Содержание программы охватывает вопросы, отражающие важнейшие фундаментальные понятия и определения в предметной области информационной безопасности, и опирается на изученные в рамках подготовки бакалавров по направлению 590100 «Информационная безопасность» следующих дисциплин из базовой части профессионального цикла:

1. Программно-аппаратные средства защиты информации;
2. Организационное и правовое обеспечение информационной безопасности;
3. Техническая защита информации;
4. Управление информационной безопасностью

Раздел I. Программно-аппаратные средства защиты информации

1. Классификация уязвимостей компьютерных систем. Основные пути осуществления несанкционированного доступа. Объекты защиты в компьютерной системе.

2. Идентификация и аутентификация пользователя. Взаимная проверка подлинности пользователей. Методы аутентификации: общая характеристика

функции аутентификации; аутентификация на знании; аутентификация на основе обладания предметом; аутентификация на воплощенных характеристиках. Протоколы аутентификации.

3. Методы реализации контроля и разграничения доступа: общая характеристика функции контроля и разграничения доступа; способы контроля и управления доступом; механизмы контроля и разграничения доступа. Концепция построения систем разграничения доступа (СРД).

4. Показатели защищенности автоматизированных систем. Требования к классам средств вычислительной техники и коммутационного оборудования.

5. Оценочный уровень доверия. Средства и методы анализа программного обеспечения на наличие недекларированных возможностей.

6. Средства доверенной загрузки уровня платы расширения. Средства доверенной загрузки уровня расширения базовой системы ввода-вывода. Средства доверенной загрузки уровня загрузочной записи. Совместное применение средств доверенной загрузки и средств защиты информации от несанкционированного доступа.

7. Статические методы защиты от несанкционированного копирования. Динамические методы защиты от несанкционированного копирования. Программные и аппаратные реализации систем защиты от копирования. Ключи HASP. Системы защиты от несанкционированного использования. Сеансовое лицензирование программного обеспечения.

8. Ключевая подсистема криптосистемы: строение и порядок ключевого множества; генерация ключей; обеспечение секретности ключей; протоколы обмена ключами; стойкость к компрометациям; архитектура ключевых систем; особенности ключевых систем для защищенного хранения данных.

9. Защита программ от исследования. Обфускация. Встраивание неисполняемых кусков кода. Метод самогенерации кода. Шифрование участков кода.

10. Компьютерные вирусы: общее описание, видовая классификация, принципы функционирования. Методы и средства антивирусной защиты. Защита от вирусов в статике процессов. Защита от вирусов в динамике процессов.

Раздел II. Организационное и правовое обеспечение информационной безопасности

1. Функции и полномочия государственных органов управления информационной безопасностью в КР.

2. Основные законодательные и подзаконные правовые акты, регулирующие процессы защиты информации в КР: законы, указы и распоряжения Президента КР, постановления и распоряжения Правительства КР, руководящие документы и стандарты.

3. Государственная тайна. Черты, характеризующие государственную тайну. Деятельность государства, обеспечивающая защиту государственной тайны. Порядок засекречивания и рассекречивания сведений, документов и

продукции. Ответственность за разглашение государственной тайны и невыполнение правил ее защиты; утрату носителей информации.

4. Коммерческая тайна: признаки, объекты защиты, режим. Перечни информации, которая не может быть отнесена к коммерческой тайне, коммерческой тайны. Ответственность за разглашение коммерческой тайны, утрату носителей информации.

5. Профессиональная тайна: критерии, виды, правовое регулирование. Служебная тайна. Требования к информации, отнесенной к служебной тайне. Информация, которая не может составлять служебную тайну. Ответственность за разглашение служебной и профессиональной тайны утрату носителей информации.

6. Информационные права человека и гражданина, закрепленные в Конституции РФ. Защита права на неприкосновенность частной жизни. Персональные данные как особый институт охраны прав на неприкосновенность частной жизни: правовые основы, субъекты права, обработка персональных данных. Классификация персональных данных п характеру: опознавательные, специальные.

7. Основные виды локальных нормативных актов (ЛНА) предприятия, обеспечивающие информационную безопасность.

8. Организационные защиты информации на предприятии: направления, принципы, условия, силы, средства. Роль руководителей в системе организационной защиты информации. Структурные подразделения, обеспечивающие информационную безопасность предприятия: задачи, функции.

9. Направления и методы, этапы работы с персоналом, обладающим конфиденциальной информацией.

Раздел III. Техническая защита информации

1. Классификация технических каналов утечки информации. Основные технические каналы утечки речевой информации, видовой информации, утечки информации при передаче ее по каналам связи, утечки информации, обрабатываемой ТСПИ.

2. Классификацию средств акустической разведки. Классификация микрофонов. Основные характеристики микрофонов. Конструкции и принципы действия электродинамических, электростатических, электромагнитных микрофонов. Принципы действия направленных микрофонов, электронных стетоскопов, радиомикрофонов и лазерных микрофонов.

3. Классификацию средств радио- и радиотехнической разведки. Общие принципы работы сканирующих компьютерных радиоприемников, радиопеленгаторов, анализаторов спектра, радиочастотомеров и многофункциональных комплектов для выявления каналов утечки информации.

4. Основные способы прослушивания телефонных переговоров. «Атаки» на компьютеризованные телефонные системы. Утечка информации в сетях сотовой связи.

5. Контроль доступа к защищаемым помещениям. Охрана оборудования и перемещаемых носителей информации. Системы защиты территории и помещений. Инженерные средства защиты периметра.

6. Основные способы и средства защиты от побочных электромагнитных излучений. Экранирование технических средств. Заземление технических средств. Фильтрация информационных сигналов. Пространственное и линейное зашумление. Способы предотвращения утечки информации через ПЭМИН ПК.

7. Особенности слаботочных линий и сетей как каналов утечки информации. Рекомендуемые схемы подключения анализаторов к электросиловым и телефонным линиям в здании. Устройства контроля и защиты проводных линий от утечки информации.

8. Основные способы и средства защиты информации в телефонных системах. Аналоговое преобразование. Цифровое шифрование. Универсальные средства защиты. Скремблеры.

9. Принципы работы металлодетекторов низкой и сверхнизкой частот, металлодетекторов с импульсной индукцией. Модель радиолокационного наблюдения в условиях нелинейной локации. Технология нелинейной локации. Эффект затухания.

10. Организационная структура системы аттестации объектов информатизации. Порядок проведения аттестации объектов информатизации. Технический контроль эффективности мер защиты информации. Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ. Методы испытаний.

Раздел IV. Управление информационной безопасностью

1. Основные положения стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности». Стандарты на отдельные процессы управления ИБ и оценку безопасности ИТ. Отраслевые стандарты в области управления ИБ.

2. Понятия политики обеспечения ИБ и политики ИБ организации. Причины выработки политики ИБ. Основные требования и принципы, учитываемые при разработке и внедрении политики ИБ. Содержание политики ИБ. Жизненный цикл политики ИБ. Ответственность за исполнение политики ИБ.

3. Необходимость управления обеспечением ИБ организации. Деятельность по обеспечению ИБ организации как процесс. Определение управления ИБ организации. Система управления ИБ организации. Процессный подход в рамках управления ИБ. Работа с процессами СУИБ организации. Стратегии построения и внедрения СУИБ.

4. Идентификация рисков ИБ. Идентификация активов. Идентификация угроз ИБ. Идентификация существующих средств управления рисками ИБ.

Идентификация уязвимостей. Идентификация последствий. Количественная оценка рисков ИБ. Оценка последствий. Оценка вероятностей. Определение уровня (величины) рисков ИБ. Оценивание рисков ИБ. Подходы к оценке рисков ИБ.

5. Снижение риска ИБ. Сохранение риска ИБ. Избежание риска ИБ. Передача риска ИБ. Принятие рисков ИБ. Коммуникация рисков ИБ. Мониторинг и пересмотр рисков ИБ.

5. ФОРМА ПРОВЕДЕНИЯ ВТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Междисциплинарный экзамен проводится устно.

6. КРИТЕРИИ ОЦЕНКИ РЕЗУЛЬТАТОВ ВТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Оценка ответов поступающего осуществляется по 100 бальной шкале.

7. ЛИТЕРАТУРА, РЕКОМЕНДУЕМАЯ ПРИ ПОДГОТОВКЕ К ВСТУПИТЕЛЬНОМУ ИСПЫТАНИЮ

а) Основная литература

Программно-аппаратные средства защиты информации

1. Платонов В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей [Текст]: учебное пособие для вузов / В. В. Платонов, 2013. – 240 с.

2. Хорев П. Б. Программно-аппаратная защита информации [Текст]: учебное пособие для вузов / П. Б. Хорев, 2015. – 352 с.

Организационное и правовое обеспечение информационной безопасности

3. Организационно-информационное обеспечение безопасности [Текст]: учебное пособие для студ. высш. учеб. заведений / А.А. Стрельцов и др. под ред. А.А. Стрельцова – М. : изд. Центр «Академкнига», 2012. – 256 с.

Техническая защита информации

4. Технические средства и методы защиты информации [Текст]: учебное пособие для вузов / ред.: А. П. Зайцев, А. А. Шелупанов. – [4-е изд., испр. И доп.]. – М. : Горячая линия-Телеком, 2013. – 616 с.

Управление информационной безопасностью

5. Башлы, П. Информационная безопасность [Текст]: учебное пособие / П. Башлы. – Ростов н/Д. : Феникс, 2010. – 253 с.

б) Дополнительная литература

Программно-аппаратные средства защиты информации

6. Грушо А. А. Теоретические основы компьютерной безопасности [Текст]: учебное пособие для вузов / А. А. Грушо, 2009. – 272 с.

7. Гашков С. Б. Криптографические методы защиты информации [Текст]: учебное пособие для вузов / С. Б. Гашков, 2010. – 304 с.

Организационное и правовое обеспечение информационной безопасности

9. Хорев, А. А. Техническая защита информации [Текст]: в 3-х т. / А.А. Хорев Т. 1 : Технические каналы утечки информации. – М. : Аналитика, 2008. – 436 с.

Управление информационной безопасностью

10. Ярочкин, В. И. Информационная безопасность [Текст]: учебник / В. И. Ярочкин. - М. : Академический проект, 2008. - 544 с.

в) Интернет-источники *(с указанием названия, авторов (владельцев ресурса, обладателей авторских прав), года публикации (размещения), режима доступа (URL).*

11. ЭБС «Университетская библиотека онлайн». URL: www.biblioclub.ru

Директор института магистратуры		Ч.К. Сыдыкова
Начальник учебно-информационного управления		Р.А. Жумабаев
Зав. кафедрой ОБИС		А.А. Абдулаев