

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ  
«БЕЛОРУССКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ СВЯЗИ»

**Программа вступительных испытаний в магистратуру для специальности:**

1-98 80 03 «Аппаратное и программно-техническое обеспечение  
информационной безопасности»

Программа вступительных испытаний в магистратуру составлена на основании учебных программ по дисциплинам «Основы теории информации», «Основы защиты информации», «Основы алгоритмизации и программирования» первой ступени высшего образования.

**СОСТАВИТЕЛИ:**

В.И.Новиков, к.т.н., доцент кафедры «инфокоммуникационных технологий»  
О.К.Барановский, к.ф.м.н, доцент кафедры «инфокоммуникационных технологий»  
Е.В.Новиков, профессор кафедры «инфокоммуникационных технологий»

## ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Настоящая программа является минимальной для подготовки к сдаче вступительных испытаний в учреждении образования «Белорусская государственная академия связи» для получения высшего образования II ступени по специальности 1-98 80 03 «Аппаратное и программно-техническое обеспечение информационной безопасности».

Программа базируется на программах вузовских дисциплин по основам защиты информации для специальностей: инфокоммуникационные технологии, сети телекоммуникаций, инфокоммуникационные системы, по основам теории информации для специальностей: инфокоммуникационные технологии, сети телекоммуникаций, инфокоммуникационные системы, почтовая связь и по основам алгоритмизации и программирования для специальности: почтовая связь.

## СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

### 1. Основы теории информации

Тема 1. Терминология. Этапы развития теории информации. Виды информации (данные, информация, знания) и их взаимосвязь. Семиотический аспект анализа концепции информации: синтаксический, семантический и прагматический аспекты. Оценка количества информации как меры снижения неопределенности об объекте или явлении. Понятие энтропии.

Тема 2. Формы представления информации. Сигнал, знак, слово, предложение, данные, знания. Виды сообщений (аналоговые, дискретные по времени и уровню сигналы).

Тема 3. Сортировка информации. Одномерные и многомерные структуры.

Тема 4. Сортировка информации. Упорядочивание информации. Техника семафоров. Разработка алгоритмов обработки одномерных структур. Разработка алгоритмов прямых (неоптимизированных) процедур упорядочивания. Применение семафоров в управлении упорядочиванием информации.

Тема 5. Представление графической информации. Растровая графика. Понятие пиксела. RGB палитра. Графические форматы. Алгоритмы сжатия. Цель сжатия данных и типы систем сжатия. Сжатие без потерь информации. Сжатие с потерей информации. Эффект пастеризации. Методы кодирования. Метод сжатия Лемпела – Зива - Вейча. Стандарты JPEG, GIF, TIFF. PhotoShop. Многослойная структура. Инструменты. Векторная графика. CorelDraw.

Тема 6. Характеристики и модели каналов передачи информации. Кодирование и модуляция. Модель системы передачи информации и ее элементы: источник сообщения, кодер источника, кодер канала, модулятор,

канал связи, приемник, демодулятор, декодер канала, декодер источника. Цель кодирования. Понятие о модуляции. Основные методы непрерывной и дискретной модуляции. Классификация сигналов и методов модуляции. Методы амплитудной и частотной модуляции. Импульсные и цифровые методы модуляции.

Тема 7. Введение в криптографию. Защита информации при передаче по каналам связи. Скремблеры. Понятие криптоанализа. Правило Керкхоффа. Современные стандарты криптосистем. Принцип симметричного шифрования с секретным ключом. Шифры перестановок. Шифры замены. Поточное шифрование. Защита каналов связи. Шифр Цезаря. Схема Вижинера. Скремблеры. Скремблеры на регистрах и датчиках псевдослучайных чисел.

Тема 8. Блочные алгоритмы. Сети Фейстеля. Алгоритм DES. ГОСТ 28147-89. Асимметричные алгоритмы RSA. Электронная цифровая подпись Асимметричные криптосистемы. Базовые определения. Алгоритм RSA. Технологии цифровых подписей. Национальный алгоритм выработки и проверки ЭЦП. Передача информации по оптическим каналам связи. Одномодовое многомодовое, ступенчатое градиентное волокно с параболическим профилем. Прослушивание оптоволокну. Микро и макроизгибы. Методы защиты от прослушивания.

## **2. Основы защиты информации**

Тема 1. Введение в защиту информации. Охраняемая информация. Терминология в сфере защиты информации. Цель, задачи и предмет защиты информации. Понятие охраняемой информации и охраняемых сведений. Категории охраняемых сведений.

Тема 2. Классификация угроз информационной безопасности и методов защиты информации. Понятие угрозы. Классификация угроз по виду, источнику характеру воздействия на объект информации. Классификация методов защиты информации.

Тема 3. Правовое обеспечение защиты информации. Государственное регулирование в сфере защиты информации. Понятие и содержание нормотворческой, исполнительной и правоприменительной деятельности. Основные нормативные правовые акты Республики Беларусь в сфере защиты информации. Состав государственной системы защиты информации Республики Беларусь. Первоочередные мероприятия по реализации государственной политики информационной безопасности. Организационно-технические мероприятия по защите информации.

Тема 4. Политика информационной безопасности. Общие сведения. Модель угроз. Управление доступом. Механизмы защиты. Принципы реализации политики безопасности.

Тема 5. Защита информации в сетях передачи данных. Общие сведения об атаках. Технологии обнаружения. Методы анализа информации при обнаружении атак. Межсетевые экраны. Детекторы вторжений.

Тема 6. Основы построения криптосистем. Основы криптографической защиты информации. Симметричные криптосистемы. Асимметричные криптосистемы.

Тема 7. Электронная цифровая подпись. Общие сведения. Однонаправленные хэш-функции. Стандарты электронной цифровой подписи и функции хеширования.

Тема 8. Аутентификация пользователей в телекоммуникационных системах. Общие сведения. Удаленная аутентификация пользователей. Протоколы идентификации с нулевой передачей знаний.

Тема 9. Мировые тренды в обеспечении информационной безопасности. Перспективные методы и технологии защиты информации. Защита национальной киберинфраструктуры. Центры реагирования на инциденты информационной безопасности. Концепция нулевого доверия. Ложные информационные системы. Технологии динамической защиты.

Тема 10. Демаскирующие признаки. Первичные и вторичные демаскирующие признаки. Классификация демаскирующих признаков.

Тема 11. Классификация технических каналов утечки информации. Понятие технического канала утечки информации. Классификация технических каналов утечки информации по физическим принципам возникновения. Акустические каналы. Электромагнитные каналы. Визуально-оптические и материально-вещественные каналы.

Тема 12. Пассивные и активные методы защиты. Экранирование электромагнитных полей. Фильтрация. Звукоизоляция помещений. Акустическая маскировка. Электромагнитная маскировка. Обнаружение и подавление закладных устройств.

Тема 13. Категорирование объектов. Средства защиты. Основные принципы категорирования объектов. Краткая характеристика объектов разных категорий. Категорирование помещений на территории объекта. Классификация инженерных ограждений. Особенности защиты въездных ворот на объект, дверных и оконных проемов. Особенности использования технических средств при охране периметра и помещений объекта. Радиоволновые и радиолучевые средства обнаружения. Оптические средства обнаружения. Сейсмические средства обнаружения. Магнитометрические средства обнаружения. Назначение и состав оборудования охранного телевидения. Структура системы. Способы представления визуальной информации оператору. Назначение и состав оборудования системы контроля и управления доступом. Структура системы. Классификация систем по количеству точек доступа. Управляемые преграждающие устройства.

### **3. Основы алгоритмизации и программирования**

Тема 1. Информация и ее измерение. Актуальность и особенности применения вычислительных средств в организации работы предприятия связи. Количество и качество информации. Структурная, статистическая и

семантические меры информации. Информация и энтропия. Сообщение и носитель информации. Каналы связи. Мера количества информации, информационное содержание.

Тема 2. Способы представления и обработки информации. Сигналы, их информационные параметры. Символы и алфавит. Аналоговое и цифровое представление информации. Дискретизация и квантование сигнала. Тактовая частота и разрядность при дискретизации. Понятие цифрового сигнала. Кодирование информации. Способы представления целых и вещественных чисел и операции над ними. Представление символьных данных

Тема 3. Информационные системы. Общая структура системы сбора и обработки информации. Классификация информационных систем. Подсистемы аналого-цифрового, цифро-аналогового преобразования, процессорной обработки и хранения информации. Организация передачи данных. Корпоративные информационные системы.

Тема 4. Информационный процесс и информационная технология. Информационный процесс в автоматизированных системах. Фазы преобразования информации. Информационные ресурсы. Понятие «информационная технология». Базы данных и базы знаний. Особенности новых информационных технологий. Обработка информации в реальном времени и в режиме пакетной обработки.

Тема 5. Основы алгоритмизации и структурного программирования. Основные понятия технологии проектирования. Жизненный цикл программного обеспечения. Информационное и организационное обеспечение. Основные этапы компьютерного решения задач. Алгоритм и его свойства. Разновидности структур алгоритмов. Способы описания алгоритмов. Стандартизация графического представления алгоритмов. Реализация основ структурного программирования в языках программирования.

Тема 6. Программное обеспечение эксплуатации компьютерных систем. Операционные системы. Классификация программного обеспечения. Характеристика основных видов программного обеспечения. Понятие операционной системы. Классификация операционных систем. Тенденция развития операционных систем. Сетевые операционные системы. Управление памятью в многозадачных и многопользовательских ОС, виртуальная память и файл подкачки. Особенности ОС семейства Windows. Системы разработки. Прикладное программное обеспечение.

Тема 7. Программное обеспечение технологий обработки информации. Интегрированный пакет Microsoft Office. Структура и назначение. Организация взаимодействия между основными компонентами пакета, их возможности и области применения. Операционная среда и графический интерфейс, обеспечивающий систему обработки информации. Совместное использование компонент MicrosoftOffice. Шаблоны. Концепция баз данных в Excel.

Тема 8. Основы объектно-ориентированного программирования. Основные понятия объектно-ориентированного программирования. Особенности использования объектов. Свойства и методы. Коллекции.

Обработка ошибок. Объекты. Классы. Инкапсуляция, наследование, полиморфизм.

Тема 9. Введение в язык Visual Basic for Application. Основные элементы языка. Типы данных. Операции и их приоритет. Выражения. Основные операторы. Работа со строками, датами и временем. Реализация основ структурного программирования в Visual Basic for Application. Объекты приложений MS Office. Организация взаимодействия с основными видами объектов приложений интегрированного пакета. Интегрированная среда разработки.

Тема 10. Программирование интерфейса приложений. Понятие об окнах сообщений. Вывод и ввод информации с помощью стандартных функций. Диалоговые окна. Технология создания элементов управления: текстовые поля, надписи, флажки, переключатели, списки, кнопки управления, элементы управления ActiveX. Технология создания меню и панелей инструментов.

Тема 11. Сетевые информационные технологии. Классификация компьютерных сетей. Реализации интерфейсов локальных сетей. Структура и технические средства локальных сетей. Мост, концентратор, шлюз. Понятие протокола передачи информации. Сетевое программное обеспечение.

## РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Новыш, Б. В. Теория информации: Пособие / Б. В. Новыш, Д.В.Шаститко. – Мн.: Акад. упр. при Президенте Респ. Беларусь, 2011. – 139 с.
2. Панин, В.В. Основы теории информации: учеб. пособие для вузов / В.В. Панин – М.: Бином, 2007. – 437 с.
3. Курмашев В.И., Новиков В.И., Чубаров С.И. Криптография и основы защиты коммерческой информации – Минск, из-во МИУ, 2013г. Электронный учебник.
4. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации / Учебное пособие для студентов высших учебных заведений. – М.: Академия, 2006. – 256 с.
5. Торокин, А.А. Инженерно-техническая защита информации / А. А. Торокин. – М. : Гелиос АРВ, 2005. – 960 с.
6. Магауенов, Р.Г. Системы охранной сигнализации: основы теории и принципы построения : учеб. пособие / Р. Г. Магауенов. – М. : Горячая линия – Телеком, 2004. – 367 с.
7. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий. М.: НИУ ВШЭ, 2011.
8. Рябко, Б.Я. Криптографические методы защиты информации: учебное пособие для студентов вузов // Б.Я. Рябко, А.Н. Фионов - М.: Горячая линия-Телеком, 2005. - 229 с.
9. Грибунин В.Г. Комплексная система защиты информации на предприятии.– М.: Академия, 2009. – 415 с.
10. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В. Ф. Шаньгин. – М. : Издат. дом «Форум»: Инфра-М, 2011. – 416 с.
11. Указ Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь»
12. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»
13. Информатика: Учебник /под ред. Проф. Н.В.Макаровой - М.: Финансы и статистика.
14. А.Н.Терехов. Технология программирования. - БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий - ИНТУИТ.ру.
15. Гарнаев А.Ю. Самоучитель VBA – 2-е издание, перераб. и доп. – Спб.: БХВ-Петербург, 2007. – 560 с.: ил.
16. А.Ананьев, А.Федоров. Самоучитель Visual Basic 6.0. – СПб.: БХВ – Санкт-Петербург.
17. О.Д. МЕРДИНА, Е.В. СТЕЛЬМАШОНОК. Проектирование WINDOWS – приложений на VISUAL BASIC .Учебное пособие: СПб., СПбГИЭУ.
18. Слепцова Л.Д. Программирование на VBA в Microsoft Office 2010. Самоучитель. : – М: Издательский дом "Диалектика", "Вильямс", 2010– 432 с.

## Критерии оценки вступительного испытания

**10 (десять) баллов** заслуживает абитуриент, обнаруживший:

систематизированные, глубокие и полные знания по всем разделам программы вступительного испытания, а также по основным вопросам, выходящим за ее пределы;

точное использование научной терминологии (в том числе на иностранном языке), грамотное, логически правильное изложение ответа на вопросы;

безупречное владение инструментарием общепрофессиональных и специальных учебных дисциплин, умение его эффективно использовать в постановке и решении научных и профессиональных задач;

выраженная способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации;

полное и глубокое усвоение основной, и дополнительной литературы программы;

умение свободно ориентироваться в теориях, концепциях и направлениях общепрофессиональных и специальных учебных дисциплин и давать им аналитическую оценку, использовать научные достижения других дисциплин;

высокий уровень культуры исполнения заданий.

**9 (девять) баллов** заслуживает абитуриент, обнаруживший:

систематизированные, глубокие и полные знания по всем разделам программы вступительного испытания;

точное использование научной терминологии (в том числе на иностранном языке), грамотное, логически правильное изложение ответа на вопросы;

владение инструментарием общепрофессиональных и специальных учебных дисциплин, умение его эффективно использовать в постановке и решении научных и профессиональных задач;

способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации в рамках программы вступительного испытания;

полное усвоение основной и дополнительной литературы, рекомендованной программой вступительного испытания;

умение ориентироваться в теориях, концепциях и направлениях общепрофессиональных и специальных учебных дисциплин и давать им аналитическую оценку;

высокий уровень культуры исполнения заданий.

**8 (восемь) баллов** заслуживает абитуриент, обнаруживший:

систематизированные, глубокие и полные знания по всем разделам программы вступительного испытания;

использование научной терминологии (в том числе на иностранном языке), грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения;

владение инструментарием общепрофессиональных и специальных учебных дисциплин (методами комплексного анализа, техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач;

способность самостоятельно решать сложные проблемы в рамках программы вступительного испытания;



усвоение основной и дополнительной литературы, рекомендованной программой вступительного испытания;

умение ориентироваться в теориях, концепциях и направлениях общепрофессиональных и специальных учебных дисциплин и давать им аналитическую оценку;

высокий уровень культуры исполнения заданий.

**7 (семь) баллов** заслуживает абитуриент, обнаруживший:

систематизированные, глубокие и полные знания по всем разделам программы вступительного испытания;

использование научной терминологии (в том числе на иностранном языке), грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения;

владение инструментарием общепрофессиональных и специальных учебных дисциплин, умение его использовать в постановке и решении научных и профессиональных задач;

свободное владение типовыми решениями в рамках программы вступительного испытания;

усвоение основной и дополнительной литературы, рекомендованной программой вступительного испытания;

умение ориентироваться в основных теориях, концепциях и направлениях общепрофессиональных и специальных учебных дисциплин и давать им аналитическую оценку;

высокий уровень культуры исполнения заданий.

**6 (шесть) баллов** заслуживает абитуриент, обнаруживший:

достаточно полные и систематизированные знания в объеме программы вступительного испытания;

использование необходимой научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать обобщения и обоснованные выводы;

владение инструментарием общепрофессиональных и специальных учебных дисциплин, умение его использовать в решении профессиональных задач;

способность самостоятельно применять типовые решения в рамках программы вступительного испытания;

усвоение основной литературы, рекомендованной программой вступительного испытания;

умение ориентироваться в базовых теориях, концепциях и направлениях общепрофессиональных и специальных учебных дисциплин и давать им сравнительную оценку;

высокий уровень культуры исполнения заданий.

**5 (пять) баллов** заслуживает абитуриент, обнаруживший:

достаточные знания в объеме программы вступительного испытания;

использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;

владение инструментарием общепрофессиональных и специальных учебных дисциплин, умение его использовать в решении профессиональных задач;

способность самостоятельно применять типовые решения в рамках программы вступительного испытания;

усвоение основной литературы, рекомендованной программой вступительного испытания;

умение ориентироваться в базовых теориях, концепциях и направлениях общепрофессиональных и специальных учебных дисциплин и давать им сравнительную оценку;

достаточный уровень культуры исполнения заданий.

**4 (четыре) балла** заслуживает абитуриент, обнаруживший:

достаточный объем знаний в рамках программы вступительного испытания;

усвоение основной литературы, рекомендованной программой вступительного испытания;

использование научной терминологии, логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок;

владение инструментарием общепрофессиональных и специальных учебных дисциплин, умение его использовать в решении стандартных (типовых) задач;

умение решать стандартные (типовые) задачи;

умение ориентироваться в основных теориях, концепциях и направлениях общепрофессиональных и специальных учебных дисциплин и давать им оценку;

допустимый уровень культуры исполнения заданий.

**3 (три) балла** выставляется абитуриенту, обнаружившему:

недостаточно полный объем знаний в рамках программы вступительного испытания;

знание части основной литературы, рекомендованной программой вступительного испытания;

использование научной терминологии, изложение ответа на вопросы с существенными, логическими ошибками;

слабое владение инструментарием общепрофессиональных и специальных учебных дисциплин, некомпетентность в решении стандартных (типовых) задач;

неумение ориентироваться в основных теориях, концепциях и направлениях общепрофессиональных и специальных учебных дисциплин;

низкий уровень культуры исполнения заданий.

**2 (два) балла** – фрагментарные знания в рамках программы вступительного испытания;

знания отдельных литературных источников, рекомендованных программой вступительного испытания;

неумение использовать научную терминологию программы, наличие в ответе грубых, логических ошибок;

низкий уровень культуры исполнения заданий.

**1 (один) балл** – отсутствие знаний и компетенций в рамках программы вступительных испытаний или отказ от ответа.