**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ**
**Государственное образовательное учреждение**
**высшего профессионального образования**
**«Башкирский государственный педагогический университет**
**им. М. Акмуллы»**
**(ГОУ ВПО «БГПУ им. М.Акмуллы»)**

_____СОГЛАСОВАНО _____УТВЕРЖДАЮ

«_____» _____ 200__г «_____» _____ 200__г.

**УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС**

**Теология по направлению 033400**
**Программа дисциплины**

# Современные информационные технологии в общественной деятельности (ФГОСТ ВПО 010300 Фундаментальная информатика и информационные технологии)

**Квалификации (степени) выпускника: магистр**

## ПОЯСНИТЕЛЬНАЯ ЗАПИСКА.

Курс «Современные информационные технологии в общественной деятельности» принимает непосредственное участие в профессиональной подготовке специалистов в педагогической, правовой областях, в сфере здравоохранения, культуры, искусства, журналистики, управления, социальной работы, в военной области, управленцев, экономистов, философов, историков, юристов, политологов, социологов, психологов, врачей, искусствоведов, педагогов библиотекарей, работников правоохранительных органов и др.

### 1. ЦЕЛИ И ЗАДАЧИ:

**Цель:** Формирование этических и эстетических компонентов информационной культуры.

В ходе ее достижения решаются следующие задачи: овладение основами современных информационных технологий, и их практическое применение в общественной жизни, воспитание культуры рациональных методов оперирования знаниями.

### 2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОСНОВНЫХ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ МАГИСТРАТУРЫ

**Выпускник должен обладать следующими общекультурными компетенциями (ОК):**

способностью понимать и анализировать мировоззренческие социально и личностно значимые философские проблемы (ОК-1);

способностью совершенствовать и развивать свой интеллектуальный и общекультурный уровень, добиваться нравственного и физического совершенствования своей личности (ОК-2);

готовностью к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности (ОК-3);

способностью свободно пользоваться русским и иностранными языками, как средством делового общения (ОК-4);

способностью использовать на практике навыки и умения в организации исследовательских и проектных работ, в управлении коллективом (ОК-5)

готовностью проявлять инициативу, в том числе в ситуациях риска брать на себя всю полноту ответственности (ОК-6);

способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и изменения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности (ОК-7);

способностью к профессиональному использованию оборудования и приборов (в соответствии с магистерской программы) (ОК-8);

способностью демонстрировать навыки самостоятельной научно-исследовательской работы и работы в научном коллективе, способность порождать новые идеи (ОК-9);

способностью использовать углубленные знания правовых и этических норм при оценке последствий свой профессиональной деятельности, при разработке и осуществлении социально значимых проектов (ОК-10).

**Выпускник должен обладать профессиональными компетенциями (ПК), такими как:**

способность применять в профессиональной деятельности современные языки программирования и языки баз данных, методологии системной инженерии, системы автоматизации проектирования, электронные библиотеки и пакеты программ, современные профессиональные стандарты информационных технологий, (в соответствии с профилизацией)(ПК-1);

способностью профессионально решать задачи производственной и технологической деятельности с учетом современных достижений науки и техники, включая: разработку алгоритмических и программных решений в области системного и прикладного программирования; разработку математических, информационных и имитационных моделей по тематике выполняемых исследований; создание информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных; разработку текстов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям; разработку эргономичных человеко-машинных интерфейсов (в соответствии с профилизацией) (ПК-2);

способность разрабатывать и реализовывать процессы жизненного цикла информационных систем, программного обеспечения, сервисов систем информационных технологий, а также методы и механизмы оценки и анализа функционирования средств и систем информационных технологий; способность разработки проектной и программной документации, удовлетворяющей нормативным требованиям (ПК-3);

*научно-исследовательская деятельность:*

способность демонстрировать знания фундаментальных и смежных прикладных разделов специальных дисциплин магистерской программы,

знания общеметодологического характера, знания истории развития информатики и информационных технологий (ПК-4);

способность использовать углубленные теоретические и практические знания в области информационных технологий и прикладной математике, фундаментальные концепции и системные методологии, международные и профессиональные стандарты в области информационных технологий, а также знания, которые находятся на передовом рубеже данной науки (ПК-5);

способность разрабатывать корпоративную техническую политику развития корпоративной инфраструктуры информационных технологий на принципах открытых систем (ПК14);

способностью разрабатывать корпоративные стандарты и профили функциональной стандартизации приложений, систем, информационной инфраструктуры (ПК15);

*педагогическая деятельность:*

способность консультировать по вопросам выполнения курсовых и дипломных работ студентов высших и средних учебных заведений, выполняемых по тематике информационных технологий (ПК16);

способность проводить семинарские и практические занятия со студентами, а также лекционные занятия спецкурсов по профилю специализации (ПК17).

## 3. ОБЪЕМ КУРСА И ВИДЫ УЧЕБНОЙ РАБОТЫ.

| **Вид учебной работы** | **Всего часов** | **1 семестр** |
|---|---|---|
| Общая трудоемкость | 72 | 72 |
| Аудиторные занятия | 30 | 30 |
| Лекции | 10 | 10 |
| Практические занятия (семинары) | 4 | 4 |
| Лабораторные работы | 16 | 16 |
| Самостоятельная работа | 42 | 42 |
| Курсовые работы/рефераты | - | |
| Вид итогового контроля | | зачет |

## 4.1. РАЗДЕЛЫ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНЫХ ЗАНЯТИЙ.

## 4.2. МЕЖДИСЦИПЛИНАРНЫЕ СВЯЗИ ДИСЦИПЛИНЫ:

| № | Наименование раздела дисциплины | Распределение трудоемкости (в часах) по видам учебных занятий | | | | |
|---|---|---|---|---|---|---|
| | | ЛК | ПЗ | ЛБ | СРС | Всего |
| № | Наименование разделов дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин | № разделов данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин | | | | |
| 1. | Тема 1.1. История развития вычислительной техники. | 2 | - | 3 | | |
| 2 | 3 | 4 | | | | 5 |
| 1. | информатика | + | + | + | | + |
| 2. | технология | + | + | + | | + |
| 3. | социология | + | + | + | | + |
| 4. | Тема: 2.1. Программное обеспечение. | - | - | 2 | | 4 |
| 3. | **ТЕМА 3. Теоретические основы управления знаниями** | 2 | - | 1 | | 3 |
| | Тема: 3.1.Операционная система и обработка текстовой информации. | - | - | 4 | | 4 |
| | Тема: 3.2.Процессоры электронных таблиц. | - | - | 2 | | 4 |
| 4. | **ТЕМА 4. Информационные системы и технологии.** | 2 | - | 1 | | 3 |
| | Тема: 4.1. Системы управления базами данных (СУБД). | - | - | 2 | | 4 |
| | Тема: 4.2. Алгоритмизация и программирование. | - | - | 2 | | 4 |
| 5. | **ТЕМА 5. Информационная безопасность.** | 2 | - | - | | 3 |
| | Тема: 5.1.Организационно-правовое обеспечение защиты информации. | - | - | 2 | | 4 |
| | Тема: 5.2. Защита информации в информационных системах. | - | - | 2 | | 4 |

## 4.2. СОДЕРЖАНИЕ ЛЕКЦИОННЫХ ЗАНЯТИЙ.

**ТЕМА 1. Представление об информации (2ч.)**

Термин «информация» происходит от латинского «information», что означает «разъяснение», «осведомление», «изложение».

Существует множество определений информации. Так один из основоположников современной теории информации, Норберт Винер, определял информацию так: Информация есть информация, а не материя или энергия»

Это определение кажется достаточно полным и универсальным, однако в качестве инструмента для построения научной методологии практически невозможно. Математическая теория Клода Шеннона, позволяет вероятностно обосновать надежность передачи сигналов по линии связи. В подходе Шеннона информация – эта мера снижения неопределенности системы. Существует также термодинамический (энергетический) подход, рассматривающий информацию как способ уменьшения энтропии системы.

Советским математиком Колмогоровым был предложен алгоритмический подход, позволяющий оценить информацию по сложности алгоритма, необходимого для ее обработки. Все эти подходы тесно связывали понятие информации со сферой применения.

С позиции материалистической философии информация есть отражение реального мира с помощью сведений (сообщений). Сообщение – это форма представления информации в виде речи, текста, изображения, цифровых данных, графиков, таблиц и т.п. В широком смысле информация – это общенаучное понятие, включающее в себя обмен сведениями между людьми, обмен сигналами между живой и неживой природой, людьми и устройствами.

*Информация – это сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые уменьшают степень неопределенности и неполноты имеющихся о них знаний.*

**ТЕМА 2. Роль информации в развитии общества (2ч.)**

В истории развития цивилизации произошло несколько информационных революций – преобразований общественных отношений из-за кардинальных изменений в сфере обработки информации. Следствием подобных преобразований являлось приобретение человеческим обществом нового качества.

*Первая информационная революция* связана с появлением языка и членораздельной человеческой речи. Ведь именно развитие языка оказало колоссальное влияние на развитие сознания людей, а его использование в их практической деятельности стало информационной основой появления первых технологий, то есть знания и навыков рациональной организации этой деятельности.

В первобытном обществе использовались и распространялись только «живые знания», носителями которых являлись живые люди – старейшины, жрецы, шаманы. В этих условиях процессы накопления и распространения знания в обществе осуществлялись чрезвычайно медленно, а сохранение уже накопленных знаний было недостаточно надежным. Со смертью их носителей многие знания утрачивались и должны были формироваться заново. На это уходили столетья.

Ситуация коренным образом изменилась, когда люди научились отчуждать знания и фиксировать их на материальных носителях в виде рисунков, чертежей, словных знаков, многие из которых сохранились до настоящего времени. Это и привело ко второй информационной революции.

Вторая информационная революция связана с изобретением письменности. Это изобретение позволило не только обеспечить сохранность уже накопленных человеческим обществом знаний, но и повысить достоверность этих знаний, создать условия для их существенно более широкого, чем раннее, распространения. Это был крупнейший шаг в цивилизации, последствия которого мы ощущаем до настоящего времени. Ведь именно изобретением письменности стало возможным развитие науки и культуры в современном понимании этих терминов.

*Третья информационная революция* началась в эпоху Возрождения и связана с изобретением книгопечатания, которое следует признать одной из первых информационных технологий. Широкое внедрение этого изобретения в социальную практику привело к первому информационному взрыву. Появились первые библиотеки печатных книг, сначала частного характера, а затем публичные. Печатная книга стала главным хранителем и источником знаний.

*Четвертая информационная революция* началась в XIX веке и продолжалась 1-ую половину XX в. Тогда были изобретены и стали все более широко распространяться такие новые средства информационной коммуникации, как радио, телефон и телевидение. Эти средства оказывают значительное воздействие на формирование общественного сознания. Благодаря этим средствам люди уже не испытывают чувства одиночества и изолированности от окружающего их общества. Веди они сегодня подключены к общему информационному пространству не только своей страны, но и значительной части нашей планеты.

*Пятая информационная революция* началась в 50-е годы XX в., то есть с того времени, когда в социальной практике стали использоваться средства цифровой вычислительной техники. Применение этих средств для обработки научной, экономической и социальной информации кардинальным образом

изменило возможности человека по активизации и эффективному использованию информационных ресурсов.

Этот период характеризуют три фундаментальные инновации:

- переход от механических и электрических средств преобразования информации к электронным;
- миниатюризация всех узлов, устройств, приборов и машин;
- создание программно-управляемых устройств и процессов.

Справка о смене поколений ЭВМ

1-е поколение (начало 50-х гг.) Элементная база – электронные лампы.

2-е поколение (с конца 50-х гг.) Элементная база – полупроводниковые элементы.

3-е поколение (начало 60-х гг.) Элементная база – интегральные схемы, многослойный печатный монтаж.

4-х поколение (с середины 70-х гг.) Элементная база –микропроцессоры, большие интегральные схемы.

5 поколение (с середины 80-х гг.) Началась разработка интртеллектуальных компьютеров, пока не увенчавшаяся успехом.

*Информационная технология (ИТ) – это процесс, использующий совокупность средств и методов сбора, обработки передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса или явления.*

*Телекоммуникация* – это дистанционная передача данных на базе компьютерных сетей и современных технических средств связи.

Бурное развитие компьютерной техники и информационных технологий послужило толчком к развитию общества, пост роенного на использовании различной информации и получившего название информационного общества.

*Информационное общество – это общество в котором большинство работающих занято производством, хранением, переработкой и реализацией информации и знаний.*

Процесс информатизации общества является закономерным глобальным процессом развития цивилизации, который обусловлен целым рядом объективных факторов. Важнейшими из них являются:

- быстро возрастающая сложность искусственно создаваемой человеком среды своего обитания – техносферы, которая все больше снижает надежность и устойчивость среды;
- истощение природных ресурсов планеты и обусловленная этим необходимость отказа от господствующей в настоящее время парадигмы экстенсивного развития цивилизации;
- возрастание экологической опасности и необходимость поиска решения самой актуальной и сложной проблемы современности – проблемы выживания человечества как биологического вида.

*Информатизация общества – это организованный социально-экономический и научно-технический процесс создания оптимальных условий для*

*удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.*

**ТЕМА 3. Теоретические основы управления знаниями (2ч.)**

Управление знаний представляет собой одно из быстро развивающихся направлений информатики. Все современные достижения компьютерной индустрии, начиная от микрочипов, встроенных в бытовую технику, и заканчивая распределенными информационными системами суперкомпьютеров, так или иначе связанных с процессом получения, хранения, переработки и применения знаний. В этой теме даны теоретические основы и описаны основные технологии, позволяющие управлять знаниями.

Несмотря на то, что само определение знаний гораздо старше и шире, чем определение информации, в компьютерно-кибернетическую эпоху информации уделяется большое внимание. В конце двадцатого в начале двадцать первого века управление знаниями становится все более и более актуальным.

Во-первых, сформировался запрос к достижениям в этой области со стороны бизнеса. Возникла потребность не только в информации, но и в стандартизированном умении этой информацией пользоваться. Нужны методы и средства по извлечению, формализации, хранению и использованию знаний.

Во-вторых, в науке были открыты методы получения и формализации знаний такого рода, которые еще в середине прошлого век считались уникальными и неповторимыми сочетание потребности и возможностей неизбежно ведет к появлению новой парадигмы обработки информации в компьютерной индустрии. Эта парадигма не замедлила появиться под названием «управление знаниями» и ныне приобретает все большую популярность и широкое распространение.

Существует четырехслойная модель предметной области управления знаниями.

***Теоретическое и философское ядро*** управления знаниями составляют как философские, так и естественнонаучные труды, исследования и произведения как древних (в большей степени) так и современных мыслителей, которые старались определить само понятие «знания», классифицировать и упорядочить виды и типы знаний, способы работы со знаниями. К философско-теоретическому ядру можно отнести труды таких ученых, как Аристотель, Платон, Маршал, Маймонид, Гегель, Декарт, Кант, Риль, Хайдеггер Гадамер, Минский и другие.

К процессам управления знаниями относятся:

- *извлечение знаний*, включая создание, исследование, накопление, проверку полезности и применимости знаний;
- *организация знаний*, включая моделирование, классификацию и

интеграцию знаний;

- *поставка знаний*, включая распространение, техническую поддержку совместное и повторное использование знаний.

*Организационные, социальные и управляющие элементы* составляют третий слой четырехслойной модели. К этому слою относятся такие понятия, как знания и память организации, корпоративная культура, конкурентные преимущества, взаимодействие внутри и вне организации, интеллектуальный капитал, стратегии использования и передачи знаний, использование знаний в социальных сообществах и сетях, мотивация к использованию и созданию знаний у сообществ и индивидов, а также архитектура, интеграция и жизненный цикл системы управления знаниями.

*Поддерживающие элементы и технологии* находятся во внешнем слое, и только они непосредственно связаны с технической стороной организации и управления знаниями. К этим элементам и технологиям можно отнести:

-сетевую инфраструктуру, мобильную и кабельную;

- хранилища данных, как структурированные и интеллектуальные, так и неструктурированные индексированные (то есть в чистом виде базы данных);

- приложения, обеспечивающие семантическое и онтологическое структурирование знаний;

- системы метазнаний (экспертные системы, системы искусственного интеллекта), обеспечивающие частную или полную автоматизацию процесса управления знаниями;

- технологии извлечения и представления знаний;

- программные агенты, обеспечивающие автоматизированное накопление знаний;

Существуют и многие другие технологии, оформленные непосредственно в виде приложений пользователя или приложений среднего звена, а также аппаратное обеспечение этих технологий.

Жизненный цикл управления знаниями напоминает жизненный цикл разработки программного обеспечения. Различие состоит в том, что при каждой интеграции жизненного цикла программного обеспечения происходит улучшение функциональных возможностей программы, а при каждой итерации жизненного цикла управления знаниями происходит увеличение количества и качества знания в организации.

*Знания это выявленные закономерности предметной области (принципы, связи, законы), позволяющие решать задачи в этой области.*

Часто под знаниями понимают структурированные данные, данные о данных, или *метаданные.*

Для хранения данных используются базы данных (для них характерны большой объем и относительно удельная стоимость информации), для хранения знаний – базы знаний (небольшого объема, но исключительно дорогие информационные массивы). База знаний – основа любой интеллектуальной системы.

## ТЕМА 4. Информационные системы и технологии (2ч.)

Информационная технология обработки данных предназначена для решения хорошо структурированных задач, по которым имеются необходимые входные данные и известны алгоритмы и другие стандартные процедуры их обработки. Внедрение информационных технологий и систем на этом уровне существенно повышает производительность труда персонала, освобождает его от рутинных операций, возможно, даже ведет к необходимости сокращения численности работников.

Целью информационной технологии управления является удовлетворение информационных потребностей всех без исключения сотрудников фирмы, имеющих дело с принятием решений. Она может быть полезна на любом уровне управления.

ИС управления идеально подходят для удовлетворения сходных информационных потребностей работников различных функциональных подсистем (подразделений) или уровней управления фирмой. Поставляемая ими информация содержит сведения о прошлом, настоящем и вероятно будущем фирмы. Это информация имеет вид регулярных или специальных управленческих отчетов.

Для принятия решений на уровне управленческого контроля информация должна быть представлена в агрегированном виде так, чтобы просматривись тенденции изменения данных, причины отклонений и возможные решения. На этом решаются следующие задачи обработки данных:

- оценка планируемого состояния объекта управления;
- оценка отклонений от планируемого состояния;
- выявление причин отклонений;
- анализ возможных решений и действий.

Информационная технология управления направлена на создание различных отчетов.

*Регулярные* отчеты создаются в соответствии с установленным графиком определяющим время создания, например месячный анализ продаж компании.

*Специальные* отчеты создаются по запросам управленцев или при возникновении в компании каких-то незапланированных ситуаций.

Те и другие виды отчетов могут иметь форму суммирующих, сравнительных и чрезвычайных отчетов.

В *суммирующих* отчетах данные объединены в отдельные группы, отсортированы и представлены в виде промежуточных и окончательных итогов по отдельным полям.

*Сравнительные* отчеты содержат данные, полученные из различных источников или классифицированные по различным признакам, и используются для сравнения.

*Чрезвычайные* отчеты содержат данные исключительного (чрезвычайного) характера.

**ТЕМА 5. Информационная безопасность (2ч.)**

## 1.Защита информации

1.Основы защиты информации и сведений, составляющих государственную тайну.

Понятие «информация» сегодня употребляется весьма широко и разносторонне. Трудно найти такую область знаний, где бы оно не использовалось. Огромные информационные потоки буквально захлестывают людей. Как и всякий продукт, информация имеет потребителей, нуждающихся в ней, и потому обладает определенными потребительскими качествами, а также имеет и своих обладателей или производителей.

С точки зрения потребителя, качество используемой информации позволяет получать дополнительный экономический или моральный эффект.

С точки зрения обладателя – сохранение в тайне коммерчески важной информации позволяет успешно конкурировать на рынке производства и сбыта товаров и услуг. Это, естественно, требует определенных действий, направленных на защиту конфиденциальной информации. При этом под безопасностью понимается состояние защищенности жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз.

При хранении, поддержании и предоставлении доступа к любому информационному объекту его владелец либо уполномоченное им лицо накладывает явно либо самоочевидно набор правил по работе с ней. Умышленное их нарушение классифицируется как атака на информацию.

Каковы возможные последствия атак на информацию? В первую очередь, конечно, это экономические потери.

Раскрытие коммерческой информации может привести к серьезным прямым убыткам на рынке.

Известие о краже большого объема информации обычно серьезно влияет на репутацию фирмы, приводя косвенно к потерям в объемов торговых операций.

Фирмы-конкуренты могут воспользоваться кражей информации, если та осталась незамеченной, для того чтобы полностью разорить фирму, навязывая ей фиктивные либо заведомо убыточные сделки.

Подмена информации, как на этапе передачи, так и на этапе хранения в фирме может привести к огромным убыткам.

Многократные успешные атаки на фирму, предоставляющую какой-либо вид информационных услуг, снижают доверие к фирме у клиентов, что сказывается на объеме доходов.

Как свидетельствует отечественная и зарубежная печать, злоумышленные действия над информацией не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту.

Защита информации – комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности (целостность, доступность и, если нужно, конфиденциальность информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных).

Система называется безопасной, если она, используя соответствующие аппаратные и программные средства, управляет доступом к информации так, что только должным образом авторизованные лица или же действующие от их имени процессы получают право читать, писать, создавать и удалять информацию.

Абсолютно безопасных систем нет, поэтому говорят о надежной системе в смысле «система, которой можно доверять» (как можно доверять человеку). Система считается надежной, если она с использованием достаточных аппаратных и программных средств обеспечивает одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа.

Основными критериями оценки надежности являются политика безопасности и гарантированность.

Политика безопасности, являясь активным компонентом защиты (включает в себя анализ возможных угроз и выбор соответствующих мер противодействия), отображает тот набор законов, правил и норм поведения, которым пользуется конкретная организация при обработке, защите и распространении информации.

Выбор конкретных механизмов обеспечения безопасности системы производится в соответствии со сформулированной политикой безопасности.

Гарантированность, являясь пассивным элементом защиты, отображает меру доверия, которое может быть оказано архитектуре и реализации системы (другими словами, показывает, насколько корректно выбраны механизмы, обеспечивающие безопасность системы).

В надежной системе должны регистрироваться все происходящие события, касающиеся безопасности (должен использоваться механизм подотчетности протоколирования, дополняющийся анализом запомненной информации, то есть аудитом).

**Основные направления защиты информации**

Основные направления защиты информации – охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Сведения могут считаться государственной тайной (могут быть засекречены), если они отвечают следующим требованиям:

• соответствуют перечню сведений, составляющих государственную тайну, не входят в перечень сведений, не подлежащих засекречиванию, и отвечают законодательству РФ о государственной тайне (принцип законности);

• целесообразность засекречивания конкретных сведений установлена путем экспертной оценки вероятных экономических и иных последствий, возможности нанесения ущерба безопасности РФ, исходя из баланса жизненно важных интересов государства, общества и личности (принцип обоснованности);

• ограничения на распространение этих сведений и на доступ к ним установлены с момента их получения (разработки) или заблаговременно (принцип своевременности);

• компетентные органы и их должностные лица приняли в отношении конкретных сведений решение об отнесении их к государственной тайне и засекречивании и установили в отношении их соответствующий режим правовой охраны и защиты (принцип обязательной защиты).

Коммерческая тайна охраняется при содействии государства. Примером этого утверждения могут служить многочисленные факты ограничения доступа иностранцев в страну (в Китае – для защиты секретов производства фарфора), в отдельные отрасли экономики или на конкретные производства. В России к коммерческой тайне относили промысловую тайну, но затем она была ликвидирована как правовой институт в начале 30-х годов и в связи с огосударствлением отраслей экономики защищалась как государственная и служебная тайна. Сейчас начался обратный процесс.

Информация может составлять коммерческую тайну, если она отвечает следующим требованиям (критерии правовой охраны):

• имеет действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам;

• не подпадает под перечень сведений, доступ к которым не может быть ограничен, и перечень сведений, отнесенных к государственной тайне;

• к ней нет свободного доступа на законном основании;

• обладатель информации принимает меры к охране ее конфиденциальности.

К коммерческой тайне не может быть отнесена информация:

• содержащаяся в учредительных документах;

• содержащаяся в документах, дающих право заниматься предпринимательской деятельностью (регистрационные удостоверения, лицензии и т. д.);

• содержащаяся в годовых отчетах, бухгалтерских балансах, формах государственных статистических наблюдений и других формах годовой бухгалтерской отчетности, включая аудиторские заключения, а также в иных, связанных с исчислением и уплатой налогов и других обязательных платежей;
• содержащая сведения об оплачиваемой деятельности государственных служащих, о задолженностях работодателей по выплате заработной платы и другим выплатам социального характера, о численности и кадровом составе работающих;
• содержащаяся в годовых отчетах фондов об использовании имущества;
• подлежащая раскрытию эмитентом ценных бумаг, профессиональным участником рынка ценных бумаг и владельцем ценных бумаг в соответствии с законодательством Российской Федерации о ценных бумагах;
• связанная с соблюдением экологического и антимонопольного законодательства, обеспечением безопасных условий труда, реализацией продукции, причиняющей вред здоровью населения, другими нарушениями законодательства Российской Федерации, законодательства субъектов Российской Федерации, а также содержащая данные о размерах причиненных при этом убытков;
• о деятельности благотворительных организаций и иных некоммерческих организаций, не связанной с предпринимательской деятельностью;
• о наличии свободных рабочих мест;
• о хранении, использовании или перемещении материалов и использовании технологий, представляющих опасность для жизни и здоровья граждан или окружающей среды;
• о реализации государственной программы приватизации и об условиях приватизации конкретных объектов;
• о размерах имущества и вложенных средствах при приватизации;
• о ликвидации юридического лица и о порядке и сроке подачи заявлений или требований его кредиторами;
• для которой определены ограничения по установлению режима коммерческой тайны в соответствии с федеральными законами и принятыми в целях их реализации подзаконными актами.
Основными субъектами права на коммерческую тайну являются обладатели коммерческой тайны, их правопреемники.
Обладатели коммерческой тайны – физические (независимо от гражданства) и юридические (коммерческие и некоммерческие организации) лица, занимающиеся предпринимательской деятельностью и имеющие монопольное право на информацию, составляющую для них коммерческую тайну.

**Уровни доступа к информации с точки зрения законодательства**

Вся информация с точки зрения права делится на несколько основных сегментов:

1) Информация без ограничения права доступа. К такому рода информации, например, относится:
• информация общего пользования, предоставляемая пользователям бесплатно;
• информация о состоянии окружающей природной среды, ее загрязнении – сведения (данные), полученные в результате мониторинга окружающей природной среды, ее загрязнения (Федеральный закон от 2 мая 1997 г. № 76-ФЗ «Об уничтожении химического оружия»);
• информация в области работ по хранению, перевозке, уничтожению химического оружия – сведения о состоянии здоровья граждан и объектов окружающей среды в районах размещения объектов по хранению химического оружия и объектов по уничтожению химического оружия, мероприятиях по обеспечению химической, санитарно-гигиенической, экологической и пожарной безопасности при проведении работ по хранению, перевозке и уничтожению химического оружия, а также о мерах по предотвращению возникновения чрезвычайных ситуаций и ликвидации их последствий при выполнении указанных работ, предоставляемая по запросам граждан и юридических лиц, в том числе общественных объединений (Федеральный закон от 2 мая 1997 г. № 76-ФЗ «Об уничтожении химического оружия», статья 1.2).
Информация, содержащая сведения об обстоятельствах и фактах, представляющих угрозу жизни, здоровью граждан, не подлежит засекречиванию, не может быть отнесена к тайне.
2) Информация с ограниченным доступом – государственная тайна, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна и персональные данные как институт охраны права неприкосновенности частной жизни.
3) Информация, распространение которой наносит вред интересам общества, законным интересам и правам граждан, – порнография; информация, разжигающая национальную, расовую и другую рознь; пропаганда и призывы к войне, ложная реклама, реклама со скрытыми вставками и т. п. – так называемая «вредная» информация.
4) Объекты интеллектуальной собственности (то, что не может быть отнесено к информации с ограниченным доступом, но охраняется особым порядком через институты интеллектуальной собственности – авторское право, патентное право, средства индивидуализации и т. п. Исключение составляют ноу-хау, которые охраняются в режиме коммерческой тайны).

## Методы и средства защиты информации в компьютерных системах

Компьютерные преступления чрезвычайно многогранные и сложные явления. Объектами таких преступных посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты или программное обеспечение и базы данных, для которых технические средства

являются окружением; компьютер может выступать как предмет посягательств или как инструмент.
Виды компьютерных преступлений чрезвычайно многообразны. Это и несанкционированный доступ к информации, хранящейся в компьютере, и ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему, и разработка и распространение компьютерных вирусов, и хищение компьютерной информации. Компьютерное преступление может произойти также из-за небрежности в разработке, изготовлении и эксплуатации программно-вычислительных комплексов или из-за подделки компьютерной информации.
Среди всего набора методов защиты информации выделяют следующие:


Рисунок 11.1. Классификация методов защиты информации в компьютерных системах

**Методы и средства организационно-правовой защиты информации**

К методам и средствам организационной защиты информации относятся организационно-технические и организационно-правовые мероприятия, проводимые в процессе создания и эксплуатации КС для обеспечения защиты информации. Эти мероприятия должны проводиться при строительстве или ремонте помещений, в которых будут размещаться компьютеры; проектировании системы, монтаже и наладке ее технических и программных средств; испытаниях и проверке работоспособности компьютерной системы.
Основой проведения организационных мероприятий является использование и подготовка законодательных и нормативных документов в области информационной безопасности, которые на правовом уровне должны регулировать доступ к информации со стороны потребителей. В российском законодательстве позже, чем в законодательстве других развитых стран, появились необходимые правовые акты (хотя далеко не все).

**Методы и средства инженерно-технической защиты информации**

Инженерно-техническая защита (ИТЗ) – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

Многообразие целей, задач, объектов защиты и проводимых мероприятий предполагает рассмотрение некоторой системы классификации средств по виду, ориентации и другим характеристикам.

Например, средства инженерно-технической защиты можно рассматривать по объектам их воздействия. В этом плане они могут применяться для защиты людей, материальных средств, финансов, информации.

Многообразие классификационных характеристик позволяет рассматривать инженерно-технические средства по объектам воздействия, характеру мероприятий, способам реализации, масштабу охвата, классу средств злоумышленников, которым оказывается противодействие со стороны службы безопасности.

По функциональному назначению средства инженерно-технической защиты делятся на следующие группы:

1. физические средства, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации (рис. 16) и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий;
2. аппаратные средства – приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации. В практике деятельности предприятия находит широкое применение самая различная аппаратура, начиная с телефонного аппарата до совершенных автоматизированных систем, обеспечивающих производственную деятельность. Основная задача аппаратных средств – обеспечение стойкой защиты информации от разглашения, утечки и несанкционированного доступа через технические средства обеспечения производственной деятельности;
3. программные средства, охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбор, накопление, хранение, обработка и передача) данных;
4. криптографические средства – это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

**Физические методы и средства защиты информации**

Физические средства защиты – это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.
К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио– и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий.
Эти средства применяются для решения следующих задач:
1) охрана территории предприятия и наблюдение за ней;
2) охрана зданий, внутренних помещений и контроль за ними;
3) охрана оборудования, продукции, финансов и информации;
4) осуществление контролируемого доступа в здания и помещения.
Все физические средства защиты объектов можно разделить на три категории: средства предупреждения, средства обнаружения и системы ликвидации угроз. Охранная сигнализация и охранное телевидение, например, относятся к средствам обнаружения угроз; заборы вокруг объектов – это средства предупреждения несанкционированного проникновения на территорию, а усиленные двери, стены, потолки, решетки на окнах и другие меры служат защитой и от проникновения, и от других преступных действий (подслушивание, обстрел, бросание гранат и взрывпакетов и т. д.). Средства пожаротушения относятся к системам ликвидации угроз.

**Аппаратные методы и средства защиты информации**

К аппаратным средствам защиты информации относятся самые различные по принципу действия, устройству и возможностям технические конструкции, обеспечивающие пресечение разглашения, защиту от утечки и противодействие несанкционированному доступу к источникам конфиденциальной информации.
Аппаратные средства защиты информации применяются для решения следующих задач:
1) проведение специальных исследований технических средств обеспечения производственной деятельности на наличие возможных каналов утечки информации;
2) выявление каналов утечки информации на разных объектах и в помещениях;
3) локализация каналов утечки информации;
4) поиск и обнаружение средств промышленного шпионажа;
5) противодействие несанкционированному доступу к источникам конфиденциальной информации и другим действиям.

**Программные методы и средства защиты информации**

Системы защиты компьютера от чужого вторжения весьма разнообразны и классифицируются, как:
1) средства собственной защиты, предусмотренные общим программным обеспечением;
2) средства защиты в составе вычислительной системы;
3) средства защиты с запросом информации;
4) средства активной защиты;
5) средства пассивной защиты и другие.

**Основные направления использования программной защиты информации**

Можно выделить следующие направления использования программ для обеспечения безопасности конфиденциальной информации, в частности такие:
1) защита информации от несанкционированной доступа;
2) защита информации от копирования;
3) защита программ от копирования;
4) защита программ от вирусов;
5) защита информации от вирусов;
6) программная защита каналов связи.
По каждому из указанных направлений имеется достаточное количество качественных, разработанных профессиональными организациями и распространяемых на рынках программных продуктов.
Программные средства защиты имеют следующие разновидности специальных программ:
1) идентификации технических средств, файлов и аутентификации пользователей;
2) регистрации и контроля работы технических средств и пользователей;
3) обслуживания режимов обработки информации ограниченного пользования;
4) защиты операционных средств ЭВМ и прикладных программ пользователей;
5) уничтожения информации в защитные устройства после использования;
6) сигнализирующих нарушения использования ресурсов;
7) вспомогательных программ защиты различного назначения.

**Защита информации от несанкционированного доступа**

Для защиты от чужого вторжения обязательно предусматриваются определенные меры безопасности. Основные функции, которые должны осуществляться программными средствами, это:

1) идентификация субъектов и объектов;
2) разграничение (иногда и полная изоляция) доступа к вычислительным ресурсам и информации;
3) контроль и регистрация действий с информацией и программами.
Наиболее распространенным методом идентификации является парольная идентификация. Однако практика показывает, что парольная защита данных является слабым звеном, так как пароль можно подслушать или подсмотреть, перехватить или просто разгадать.

**Защита от копирования**

Средства защиты от копирования предотвращают использование ворованных копий программного обеспечения и являются в настоящее время единственно надежным средством – как защищающим авторское право программистов-разработчиков, так и стимулирующих развитие рынка. Под средствами защиты от копирования понимаются средства, обеспечивающие выполнение программой своих функций только при опознании некоторого уникального некопируемого элемента. Таким элементом (называемым ключевым) может быть дискета, определенная часть компьютера или специальное устройство, подключаемое к персональному компьютеру. Защита от копирования реализуется выполнением ряда функций, являющихся общими для всех систем защиты:
1. Идентификация среды, из которой будет запускаться программа (дискета или ПК);
2. Аутентификация среды, из которой запущена программа;
3. Реакция на запуск из несанкционированной среды;
4. Регистрация санкционированного копирования;
5. Противодействие изучению алгоритмов работы системы.

**Защита программ и данных от компьютерных вирусов**

Вредительские программы и, прежде всего, вирусы представляют очень серьезную опасность при хранении на ПЭВМ конфиденциальной информации. Недооценка этой опасности может иметь серьезные последствия для информации пользователей. Знание механизмов действия вирусов, методов и средств борьбы с ними позволяет эффективно организовать противодействие вирусам, свести к минимуму вероятность заражения и потерь от их воздействия.
«Компьютерные вирусы» – это небольшие исполняемые или интерпретируемые программы, обладающие свойством распространения и самовоспроизведения (репликации) в компьютерной системе. Вирусы могут выполнять изменение или уничтожение программного обеспечения или данных, хранящихся в ПЭВМ. В процессе распространения вирусы могут себя модифицировать.

**Классификация компьютерных вирусов**

В настоящее время в мире насчитывается более 40 тысяч только зарегистрированных компьютерных вирусов. Так как подавляющее большинство современных вредительских программ обладают способностью к саморазмножению, то часто их относят к компьютерным вирусам. Все компьютерные вирусы могут быть классифицированы по следующим признакам:
– по среде обитания вируса,
– по способу заражения среды обитания,
– по деструктивным возможностям,
– по особенностям алгоритма вируса.
Массовое распространение вирусов, серьезность последствий их воздействия на ресурсы компьютеров вызвали необходимость разработки и использования специальных антивирусных средств и методов их применения. Антивирусные средства применяются для решения следующих задач:
– обнаружение вирусов в КС,
– блокирование работы программ-вирусов,
– устранение последствий воздействия вирусов.
Обнаружение вирусов желательно осуществлять на стадии их внедрения или, по крайней мере, до начала осуществления деструктивных функций вирусов. Необходимо отметить, что не существует антивирусных средств, гарантирующих обнаружение всех возможных вирусов.
При обнаружении вируса необходимо сразу же прекратить работу программы-вируса, чтобы минимизировать ущерб от его воздействия на систему.
Устранение последствий воздействия вирусов ведется в двух направлениях:
– удаление вирусов,
– восстановление (при необходимости) файлов, областей памяти.
Для борьбы с вирусами используются программные и аппаратно-программные средства, которые применяются в определенной последовательности и комбинации, образуя методы борьбы с вирусами.
Самым надежным методом защиты от вирусов является использование аппаратно-программных антивирусных средств. В настоящее время для защиты ПЭВМ используются специальные контроллеры и их программное обеспечение. Контроллер устанавливается в разъем расширения и имеет доступ к общей шине. Это позволяет ему контролировать все обращения к дисковой системе. В программном обеспечении контроллера запоминаются области на дисках, изменение которых в обычных режимах работы не допускается. Таким образом, можно установить защиту на изменение главной загрузочной записи, загрузочных секторов, файлов конфигурации, исполняемых файлов и др.
При выполнении запретных действий любой программой контроллер выдает соответствующее сообщение пользователю и блокирует работу ПЭВМ.

Аппаратно-программные антивирусные средства обладают рядом достоинств перед программными:
– работают постоянно;
– обнаруживают все вирусы, независимо от механизма их действия;
– блокируют неразрешенные действия, являющиеся результатом работы вируса или неквалифицированного пользователя.
Недостаток у этих средств один – зависимость от аппаратных средств ПЭВМ. Изменение последних ведет к необходимости замены контроллера.
Современные программные антивирусные средства могут осуществлять комплексную проверку компьютера на предмет выявления компьютерных вирусов. Для этого используются такие антивирусные программы как – Kaspersky Anti-Virus (AVP), Norton Antivirus, Dr. Web, Symantec Antivirus. Все они имеют антивирусные базы, которые периодически обновляются.

**Криптографические методы и средства защиты информации**

Криптография как средство защиты (закрытия) информации приобретает все более важное значение в мире коммерческой деятельности.
Криптография имеет достаточно давнюю историю. Вначале она применялась главным образом в области военной и дипломатической связи. Теперь она необходима в производственной и коммерческой деятельности. Если учесть, что сегодня по каналам шифрованной связи только у нас в стране передаются сотни миллионов сообщений, телефонных переговоров, огромные объемы компьютерных и телеметрических данных, и все это не для чужих глаз и ушей, становится ясным: сохранение тайны этой здесь крайне необходимо.
Криптография включает в себя несколько разделов современной математики, а также специальные отрасли физики, радиоэлектроники, связи и некоторых других смежных отраслей. Ее задачей является преобразование математическими методами передаваемого по каналам связи секретного сообщения, телефонного разговора или компьютерных данных таким образом, что они становятся совершенно непонятными для посторонних лиц. То есть криптография должна обеспечить такую защиту секретной (или любой другой) информации, что даже в случае ее перехвата посторонними лицами и обработки любыми способами с использованием самых быстродействующих ЭВМ и последних достижений науки и техники, она не должна быть дешифрована в течение нескольких десятков лет. Для такого преобразования информации используются различные шифровальные средства – такие, как средства шифрования документов, в том числе и портативного исполнения, средства шифрования речи (телефонных и радиопереговоров), телеграфных сообщений и передачи данных.

**Общая технология шифрования**

Исходная информация, которая передается по каналам связи, может представлять собой речь, данные, видеосигналы, называется незашифрованными сообщениями P.
В устройстве шифрования сообщение P шифруется (преобразуется в сообщение C) и передается по «незакрытому» каналу связи. На приемной стороне сообщение C дешифруется для восстановления исходного значения сообщения P.
Параметр, который может быть применен для извлечения отдельной информации, называется ключом.
Если в процессе обмена информацией для шифрования и чтения использовать один тот же ключ, то такой криптографический процесс называется симметричным. Его основным недостатком является то, что прежде, чем начать обмен информацией, нужно выполнить передачу ключа, а для этого необходима защищенная связь.
В настоящее время при обмене данными по каналам связи используется несимметричное криптографическое шифрование, основанное на использовании двух ключей. Это новые криптографические алгоритмы с открытым ключом, основанные на использовании ключей двух типов: секретного (закрытого) и открытого.
В криптографии с открытым ключом имеются, по крайней мере, два ключа, один из которых невозможно вычислить из другого. Если ключ расшифрования вычислительными методами невозможно получить из ключа зашифрования, то секретность информации, зашифрованной с помощью несекретного (открытого) ключа, будет обеспечена. Однако этот ключ должен быть защищен от подмены или модификации. Ключ расшифрования также должен быть секретным и защищен от подмены или модификации.
Если, наоборот, вычислительными методами невозможно получить ключ зашифрования из ключа расшифрования, то ключ расшифрования может быть не секретным.
Ключи устроены таким образом, что сообщение, зашифрованное одной половинкой, можно расшифровать только другой половинкой. Создав пару ключей, компания широко распространяет открытый (публичный) ключ и надежно охраняет закрытый (личный) ключ.
Защита публичным ключом не является абсолютно надежной. Изучив алгоритм ее построения можно реконструировать закрытый ключ. Однако знание алгоритма еще не означает возможность провести реконструкцию ключа в разумно приемлемые сроки. Исходя из этого, формируется принцип достаточности защиты информации: защиту информации принято считать достаточной, если затраты на ее преодоление превышают ожидаемую стоимость самой информации. Этим принципом руководствуются при несимметричном шифровании данных.
Разделение функций зашифрования и расшифрования посредством разделения на две части дополнительной информации, требуемой для выполнения операций, является той ценной идеей, которая лежит в основе криптографии с открытым ключом.

Криптографической защите специалисты уделяют особое внимание, считая ее наиболее надежной, а для информации, передаваемой по линии связи большой протяженности, – единственным средством защиты от хищений.

## Информационная безопасность и ее основные компоненты

Под информационной безопасностью понимают состояние информационной защищенности среды общества от внутренних и внешних угроз, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств (Закон РФ «Об участии в международном информационном обмене»).
К системе безопасности информации предъявляются определенные требования:
– четкость определения полномочий и прав пользователей на доступ к определенным видам информации;
– предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы;
– сведение к минимуму числа общих для нескольких пользователей средств защиты;
– учет случаев и попыток несанкционированного доступа к конфиденциальной информации;
– обеспечение оценки степени конфиденциальной информации;
– обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя.
Под системой безопасности понимают организованную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз.
Как и любая система, система информационной безопасности имеет свои цели, задачи, методы и средства деятельности, которые согласовываются по месту и времени в зависимости от условий.

## Категории информационной безопасности

С точки зрения информационной безопасности информация обладает следующими категориями:
1. Конфиденциальность – гарантия того, что конкретная информация доступна только тому кругу лиц, для которого она предназначена; нарушение этой категории называется хищением либо раскрытием информации.
2. Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения.

3. Ааутентичность – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется фальсификацией, но уже автора сообщения.
4. Апеллируемость – довольно сложная категория, но часто применяемая в электронной коммерции – гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой; отличие этой категории от предыдущей в том, что при подмене автора, кто-то другой пытается заявить, что он автор сообщения, а при нарушении апеллируемости – сам автор пытается «откреститься» от своих слов, подписанных им однажды.

**Угрозы конфиденциальной информации**

Под угрозами конфиденциальной информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями.
Такими действиями являются:
• ознакомление с конфиденциальной информацией различными путями и способами без нарушения ее целостности;
• модификация информации в криминальных целях как частичное или значительное изменение состава и содержания сведений;
• разрушение (уничтожение) информации как акт вандализма с целью прямого нанесения материального ущерба.

*Действия, приводящие к неправомерному овладению конфиденциальной информацией:*
1. Разглашение – это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним.
2. Утечка – это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.
3. Несанкционированный доступ – это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам.

## 4.3.ПРАКТИЧЕСКИЕ ЗАНЯТИЯ 4ч. (СЕМИНАРЫ).

*Общая характеристика организации самостоятельной работы студентов под руководством преподавателя:*
Формы проведения СРСП:
- Лекционное занятие;
- Защита лабораторных работ;
- Проверка и сдача контрольных и самостоятельных работ;
- Консультации по возникшим вопросам;

- Проведение тестирования;
- Защита рефератов;
- Подведение итогов и выставление рубежного контроля.

Методические рекомендации для СРСП: изучить теоретический материал по основным вопросам к нижеуказанным темам, готовится к защите и сдаче лабораторных, самостоятельных и контрольных работ, регулярно осуществлять самоконтроль знаний.

## ТЕМА 1.1.История развития вычислительной техники (2ч.)

План

1.Первая суммирующая машина Блеза Паскаля.

2.Развитие вычислительной техники с точки зрения смены поколений компьютеров.

1. В 1642 г. франц. Математик и философ Блез Паскаль сконструировал первую суммирующую машину, которая состояла из и восьми движущихся дисков с прорезями и могла суммировать числа до восьми знаков. В 1820 г. Чарльз Калмар изобрел машину - арифмометр, которая могла производить четыре основных арифметических действия. Начало эры компьютеров связано с именем английского математика Чарльза Бэббиджа, который создал модель универсальной вычислительной машины.

2. Развитие вычислительной техники принято рассматривать с точки зрения смены поколений компьютеров:

– Первое поколение – 1945 – 1956 годы. Технические предпосылки появления первого поколения компьютеров: электронные вакуумные лампы, цифровое кодирование информации, создание устройств искусственной памяти на электростатических трубках. В компьютерах первого поколения использовался принцип фон Неймана. Низкая производительность.
– Второе поколение – 1956 – 1963 годы. Характеризуется применением для создания компьютеров транзисторов и памяти на ферритовых сердечниках, увеличением быстродействия, возникновением новых технологий программирования.
– Третье поколение – 1964 – 1971 годы. Основой послужили интегральные микросхемы, что позволило уменьшить стоимость и размеры.
– Четвертое поколение – с 1971 года и по настоящее время. Появление микропроцессора, и появление персональных компьютеров, отличительной особенностью которых стали небольшие размеры и низкая стоимость.

**ТЕМА 5.1.Организационно-правовое обеспечение защиты информации и защита информации в информационных системах (2ч.)**

План

1.Защита информации.
2. Основные направления защиты информации.
3. Методы и средства защиты информации в компьютерных системах

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий, оказывающих прямое воздействие на благополучие, а иногда и жизнь многих людей. Данная глава посвящена всестороннему рассмотрению вопросов безопасности в информационной сфере: откуда возникают угрозы безопасности и что является основанием для обеспечения надежной защиты от этих угроз.

*Информационная безопасность – это защищенность информационной среды общества посредством различных средств и методов.*

Информационная безопасность должна обеспечивать конфиденциальность, точность, полноту и доступность информации. Эффективная информационная безопасность должна основываться на теории защиты информации, в которой рассматриваются следующие направления:

- сбор, систематизация и анализ сведений о проблеме защиты информации;
- формирование на основе собранных сведений научно обоснованных прогнозов о возможности возникновения угроз;
- научно обоснованная постановка задачи защиты информации о современных условиях;
- разработка мероприятий по организации защиты информации;
- разработка методологии и инструментальной базы защиты информации. Российской Федерации был выработан ряд подходов к защите информации, закрепленный государственными документами и стандартами. Одним из таких документов является «Доктрина информационной безопасности Российской Федерации». Согласно этому документу, государственная политика обеспечения информационной безопасности основывается на следующих основных принципах:

- соблюдение Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности РФ.

- информированности общества о деятельности федеральных органов государственной власти и общественных объединений;

- правовом равенстве всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса;

- приоритетном развитии отечественных информационных и телекоммуникационных технологий, производстве технических и программных средств в целях соблюдения жизненно важных интересов РФ.

Государственная тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ.

В зависимости от вида, содержания и размеров ущерба можно выделить группы некоторых видов при утечке сведений, составляющих государственную тайну.

Политический ущерб. Экономический ущерб. Моральный ущерб.

Структура нормативной базы по вопросам информационной безопасности включает:

- Конституцию РФ;
- федеральные законы и законы РФ;
- Кодексы РФ (уголовный, гражданский, об административных правонарушения;
- постановления правительства РФ;
- ведомственные нормативные акты, ГОСТы, руководящие документы;

## 4.4. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Тема: 2.1. Программное обеспечение.

Тема: 3.1.Операционная система и обработка текстовой информации.

Тема: 3.2.Процессоры электронных таблиц.

Тема: 4.1.Системы управления базами данных (СУБД).

Тема: 4.2. Алгоритмизация и программирование.

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ.
## 5.1. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА.

**ОСНОВНАЯ:**

1.Инфороматика. Базовый курс, Под ред. С.В.Симоновича. СПб: Питер, 2000.

2.Волков В.В. Работа на персональном компьютере. Практический курс. Киев: ЮНИОР, 1999.
3.Леонтьев В., Турецкий Д. Новейшая энциклопедия программ. М.:, ОЛМА-ПРЕСС, 2002.
4.Макаров Н.В., Волков В.Б. Информатика: Учебник для вузов. – СПб.: Питер, 2011.
5.Шалин П. Windows XP. Русская и английская версия. СПб: Питер, 2002.

**Нормативно-правовые акты:**

1. Всеобщая декларация прав человека: принята и провозглашена Ген. Ассамблеей ООН 10 дек. 1948 г. - СПб.: Регион, 2004. – 13 с.

**ДОПОЛНИТЕЛЬНАЯ:**

1. Башмаков А.И., Башмакова И.А. Интеллектуальные информационные технологии. М.: издательство МГТУ им. Баумана, 2005г.
2. Вернер М. Основы кодирования. М. Техносфера, 2004.
3. Введение в информационный бизнес: Учебное пособие Под ред. В.П.Тихомирова, А.В. Хорошилова, М.: Финансы и статистика, 1996.
4. Гаврилова Т.А., Хорошевский Ф.В. Базы знаний интеллектуальных систем. СПб: Питер, 2000.
5. Гагарина Л.Г., Киселев Д.В. Федотова Е.Л. Разработка и эксплуатация автоматизированных информационных систем. М: ФОРУМ-ИФРА-М, 2007.
6. Галатенко В.А. Основы информационной безопасности. М.: Интерне – университет информационных технологий, 2006.
7. Девянин П.Н. Модели информационной безопасности компьютерных систем. М.: Издательский центр «Академия», 2005.
8. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: ТИД Диа Софт, 2002.
9. Гвоздева В.А. Лаврентьева И.Ю. Основы построения автоматизированных информационных систем. М.: ФОРУМ-ИФРА-М,2007.
10. Горлопанов В.В., Яловецкий В.И.Информационные технологии в органах государственной власти. Аналитический обзор. М.: Издательство МАГМУ, 2007.
11. Григорьев М.Н., Сергеев В.И., Уваров С.А. Логистика: информационные системы и технологии. М., Альфа-пресс, 2008.
12. Джанетто Карен, Уилер Энн. Управление знаниями. М.Добрая книга, 2005.
13. Емельянова Н.З., Партыка Т.Л. Попов И.И. Основы построения автоматизированных информационных систем. М.: ФОРУМ-ИФРА-М, 2007.
11. Желена Милан. Информационные технологии в бизнесе. СПб.: Питер, 2002.
12. Зверев Г.Н. Теоретическая информатика и ее основания (в 2 томах). М.Физматлит, 2007.

13. Кудряшов Б.Д. Теория информации: Учебник для ВУЗов. СПб.: Питер, 2009.
14. Куприянов А.И.Основы защиты информации. М.: Издательский центр «Академия», 2008.
15.Курбатов В., Скиба В. Руководство по защите от внутренних угроз информационной безопасности. СПб.: Питер, 2008.
16. Майоров С.И. Информационный бизнес: Коммерческое распространение и маркетинг. М.: Финансы и статистика, 1993.
17. Мелюхин И.С. Рынок электронных информационных продуктов и услуг в России: состояние и тенденции развития , НТ. – Серия 1. ВИНИТИ. 1994. № 2.
18. Советов Б.Я, Цехановский В.В. Информационные технологии. М.: Высшая школа, 2006.
19. Тамбовцев В.Л. Пятый рынок: экономические проблемы производства информации. М.: Изд-во МГУ, 1993.

**ВСПОМОГАТЕЛЬНАЯ**

1. Леонтьев В. П. Новейшая энциклопедия персонального компьютера 2010 – М.: ОЛМА Медиа Групп, 2010. – 800 с.
2. Старков В. Архитектура персонального компьютера: организация, устройство, работа. – М.: Горячая Линия – Телеком, 2009. – 536 с.
3. Леонов В. Самоучитель работы на компьютере. – М., 2009. – 352 с.
4. Пол Мак-Федрис. Microsoft Windows 7. Полное руководство. – М.: Вильямс, 2009. – 800 с.
5. Крис Фейли. Мастерская Windows, XP, Vista и Office. – М., 2009. – 608 с.
6. Грег Перри. Microsoft Office 2007. Все в одном.- М.: Диалектика, 2008. – 608 с.
7. Меженный О. А. Microsoft Office 2007. Краткое руководство. – М., 2009. – 384 с.
8. Джон Уокенбах. Microsoft Office Excel 2007. Библия пользователя. – М.: Диалектика, 2008. – 816 с.
9. Майкл Г., Джозеф С., Гэвин П. Microsoft Office Access 2007. Библия пользователя.- М.: Диалектика, 2008. – 1200 с.
10. Слепцова Л. Д. Программирование на VBA в Microsoft Office 2007. Самоучитель. – М., 2009. – 432 с.
11. Леонтьев В.П. Интернет 2010: Универсальный справочник – М.: Олма медиа групп, 2010. – 800 с.
12. Леонтьев В.П. Новейшая энциклопедия Интернета 2010.- М.: Олма медиа групп, 2010. – 640 с.
13. Г. Борн. Руководство разработчика на Microsoft Windows Script Host 2.0. – СПб.: Питер; М.: Изд.-торг. дом "Русская редакция", 2001. – 480 с.

14. Журавлев А.В. Персональный компьютер. Просто как дважды два. – М.: Эксмо, 2008. – 288 с.
15. Журавлев А.В. Microsoft Windows Vista. Просто как дважды два. – М.: Эксмо, 2007. – 352 с.
16. Иванова Е.Н. Microsoft Office 2007. Просто как дважды два. – М.: Эксмо, 2007. – 336 с.
17. Кушнир А.Н. Microsoft Office Access 2007. Просто как дважды два. – М.: Эксмо, 2009. – 288 с.
18. Аксак В.А. Интернет. Просто как дважды два. – М.: Эксмо, 2009. – 288 с.
19. Борисенко А.А. Локальная сеть. Просто как дважды два. – М.: Эксмо, 2009. – 192 с.

САЙТЫ ИНТЕРНЕТ-РЕССУРСОВ:

1. *www.informika.ru* – сайт Государственного научно-исследовательского института информационных технологий и теле-коммуникаций (ФГУ ГНИИ ИТТ "Информика")

2. *www.intel.ru* и *www.intel.com* – корпорация Intel

3. *www.microsoft.ru* и *www.microsoft.com* – корпорация Microsoft

4. *pcnews.ru*, *computer-news.ru* , *www.hardvision.ru, news.ferra.ru*, *www.ixbit.com*, *www.computerra.ru, www.compulenta.ru, www.comp-life.ru* – компьютерные новости

5. *www.itnews.ru*, *http://subscribe.ru/catalog/comp, www.studioit.ru*, *www.it-top.ru*, *www.cnews.ru*, *it-technologiess.ru, www.worldnewsit.ru* – новости информационных технологий

6. *www.3dnews.ru* – Daily Digital Digest, все о компьютерах – обзоры, аналитика, новости Hardware, новости Software, сети, программное обеспечение, энциклопедия и пр., тематические рассылки

7. *www.intuit.ru* – Интернет-Университет Информационных Технологий, бесплатные курсы (более 400), обучение, видеокурсы и пр.

8. *www.planet-it.ru* – портал предназначен для аккумулирования различ-ных образовательных мероприятий в области информационных тех-нологий: олимпиад, конкурсов, тестов, удаленного обучения и т.д.

9. *www.citforum.ru* – новости, рассылки и форумы по темам: IT-консалтинг, Software Engineering, программирование, СУБД, безопас-ность, Internet, сети, операционные системы, Hardware

10. *www.ict.edu.ru* – информационно-коммуникационные технологии в образовании

11. *www.forum.softweb.ru* – форум с разделами «Компьютер для начи-нающих», «Программы», «Программирование», «Интернет и сети», «Я и компьютер», группы разделов «Образование и работа», библио-тека с книгами для скачивания и пр.

12. *http://forum.oszone.net* – форум с различными группами тем в области информационных технологий

13. *www.cyberforum.ru* – форум программистов

14. *http://vbsbook.ru* – справочник по языку программирования

## 5.2. СРЕДСТВА ОБЕСПЕЧЕНИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

Единое окно доступа к образовательным ресурсам. http://window.edu.ru/

## 6. МАТЕРИАЛЬНО–ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.

Практическое осуществление обучение студентов программированию требует среды программирования, использования доменной системы БГПУ. Материально-техническая база дисциплины: новое программное обеспечение «Центра информационных компьютерных технологий».

Лекционные и практические занятия по дисциплине проводятся в новых мультимедийных компьютерных классах с использованием интерактивных досок, проекционного и мультимедийного оборудования.

В самостоятельной и аудиторной работе студентами активно испльзуется единая информационная базы (новая литература, периодика, электронные образовательные ресурсы, электронные учебники, справочники, цифровые образовательные ресурсы и др.) При освоении дисциплины для выполнения лабораторных работ необходим набор программного обеспечения: системы программирования (Turbo Pascal, Delphi, Free, Pascal).

## 7. СОДЕРЖАНИЕ ИТОГОВОГО И ПРОМЕЖУТОЧНОГО КОНТРОЛЯ

**ГРАФИК**
**промежуточного и итогового контроля**

| **№ п.п.** | **Вид контроля (выполнение лабораторных работ, тестирование.)** | **Сроки проведения** | **Перечень проверяемых дидактических единиц и компетенций** |
|---|---|---|---|
| 1. | Знание терминов и понятий, подготовка к семинарским занятиям. | | ОК, ПК |
| 2. | Выполнение лабораторных работ. | | ОК, ПК |

| | | | |
|---|---|---|---|
| **2** | **Зачет** | | **ОК, ПК** |

**ПЛАН-ГРАФИК СРС**

| **№ п.п.** | **Разделы (темы) курса** | **Задание на СРС** |
|---|---|---|
| 2. | 1-5 | Работа с материалами лекций, семинаров; дополнительной литературой; терминами, понятиями, персоналиями. |
| 3. | 1-5 | Работа с обработкой информации. Выполнение лабораторных работ. |

**ОСНОВНЫЕ ВИДЫ ЗАНЯТИЙ И ОСОБЕННОСТИ ИХ ПРОВЕДЕНИЯ.**

Основной формой ознакомления студентов с теоретическими и методологическими основами информационного знания служат практические занятия. Главный акцент на лекциях делается на разъяснении наиболее сложных тем в современном информационном пространстве и теоретической ее части. Вместе с тем, поднимаются и проблемные, дискуссионные темы, требующие рассмотрения разнообразных подходов и методов их решений. Задачей практических занятий является усвоение студентами содержания лекционных тем и углубление практических навыков работы с информацией. Основной вид практических занятий – лабораторные работы.

Лабораторные работы носят избирательный характер, проводятся по отдельным темам курса. К целям лабораторных занятий относятся активизация работы студентов в течение всего учебного процесса, формирование навыков самостоятельного поиска и анализа информации, овладение практическими навыками информационного обеспечения и владения информацией у студентов. Одной из задач семинара является организация обсуждения поставленных вопросов с вовлечением всей аудитории. Самостоятельная работа студентов носит обязательный характер и предполагает выполнение лабораторных заданий.

Осуществляется эта работа также с помощью и учетом рекомендаций преподавателя.

**7.2. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ.**

1. Дайте определение термину «информация». Каким образом измеряют информацию? Какие меры информации вам известны?
2. Как связаны между собой количество информации и мера неопределенности состояния системы?
3.Что такое «прагматическая мера информации»? Какими понятиями определяется качество информации?
4.Что такое «кодирование» и «декодирование»?
5.Что такое «классификация»? Что такое «реквизит», «классификатор»?
6. Какие системы кодирования информации применяются при классификации?
7. Расскажите об информационных революциях в истории развития цивилизации.
8. Дайте определение информационной культуре? Как она проявляется?
9. Чем определяется информационный потенциал общества?
10. Расскажите о видах ресурсов? Охарактеризуйте информационный ресурс, информационный продукт, информационную услугу. Приведите примеры?
11. Расскажите о классификации основных видов информационных услуг? Каковы составляющие рынка информационных услуг и продуктов?
12. В чем заключается правовое регулирование на информационном рынке?
13. Как вы понимаете термин «управление знаниями»?
14. Какие процессы включаются в управление знаниями?
15. Какие способы классификации знаний вы знаете?
16. Перечислите признаки интеллектуального поведения?
17. Что может быть источником данных в процессе добычи данных?
18. Что такое «получение знаний»? Какую роль этот процесс играет в инженерии знаний?
19. В чем различие инженерии знаний и управления знаниями?
20. Как вы понимаете информационную технологию?
21. Как развивались информационные системы?
22. В чем сходство и в чем различие информационной технологии и технологии материального производства?
23.Отобразите информационную технологию в виде иерархической структуры и приведите примеры ее составляющих.
24.Что такое инструментарий информационной технологии»? Как соотносятся информационная технология и информационная система?
25. Охарактеризуйте методологию использования информационной технологии.
26.Дайте общее представление об информационных технологиях обработки данных управления, автоматизации офиса, поддержки принятия решений. Назовите их основные компоненты.
27. Расскажите о компьютерных и некомпьютерных офисных технологиях.
28.Дате определение информационной безопасности.
29.Чем определяется информационная безопасность?
30. Каковы основные принципы государственной политики обеспечения информационной безопасности России?

31. Перечислите виды угроз в информационной сфере.
32. Что относится к внутренним и внешним источникам угроз информационной безопасности?
33.Дайте определение организационно-правовому обеспечению информационной безопасности. Что такое государственная тайна?
34. Какие виды ущерба может нанести нарушение Информационной безопасности?
35. Какие вы знаете угрозы информационным системам?
36. В чем заключается нарушение достоверности? Приведите пример.
37. В чем заключается нарушение конфиденциальности? Приведите пример.
38. В чем заключается нарушение целостности? Приведите пример.
39. в чем заключается нарушение доступности? Приведите пример.
40. Каким образом можно классифицировать угрозы информации? Какие способы защиты информации вам известны?

**Тематика рефератов:**
1. История развития информатики.
2. Кибернетика — наука об управлении.
3. Информатика и управление социальными процессами.
4. Информационные системы.
5. Автоматизированные системы управления.
6. Автоматизированные системы научных исследований.
7. Составные части современной информатики.
8. Построение интеллектуальных систем.
10. Информатика и естественные науки.
11. Компьютер как историогенный фактор.
12. Компьютерная революция: социальные перспективы и последствия.
13. Путь к компьютерному обществу.
14. Информатика в деятельности психолога.
15. Общие приемы правового регулирования информационных отношений.
16. Правонарушения в сфере информационных технологий.
17. Правила этикета при работе с компьютерной сетью.
18. Защита информации в Internet.
19. Системы управления базами данных.
20. Компьютерные вирусы.
21. Надежность информации.
22. Роль информатики в психологии.
23. Информатизация современного общества.
24. Физические основы ЭВМ.
25. Интернет.

**Тестовые задания для самоконтроля**
1.Для сохранения файла надо выполнить команду:
А) Пуск - Файл.
В) Файл - Сохранить как...

C) Системное меню - Сохранить.
D) Контекстное меню - Сохранить как...
E) Клавишу F5.
2. Как называется устройство ввода информации в ЭВМ непосредственно с бумажного документа?
A) Лазерные принтер;
B) Клавиатура;
C) Сканер;
D) Трекбол;
E) Джойстик.
3. Какие из ниже перечисленных программ относятся к программам - архиваторам?
A) Norton Commander;
B) ScanDisk;
C) WinRAR;
D) Mathcad Pro;
E) Corel Draw.
4 . Что такое «колонтитул»?
A) заголовок колонки документа
B) стандартный текст, помещаемей вверху или внизу каждой страницы документа
C) титульный лист документа
D) заголовок документа
E) сноска
5.Выберите команду меню для удаления всего текста (очистки) из документа?
A) ФАЙЛ, ЗАКРЫТЬ.
B) ПРАВКА, ВЫДЕЛИТЬ ВСЕ, ПРАВКА, УДАЛИТЬ.
C) Поставить курсор в начало текста, ПРАВКА, УДАЛИТЬ.
D) Поставить курсор в начало текста, нажать клавишу «DEL»
E) «Среди предъявленных ответов нет правильного»
6. По стадии обработки информация подразделяется на:
A) Переменную и постоянную;
B) Текстовую и графическую;
C) Первичную, вторичную, промежуточную и результатную;
D) Входную, выходную, внутреннюю и внешнюю;
E) Плановую, нормативно-справочную, учетную и оперативную
7.Процессор компьютера предназначен:
A) для кратковременного хранения программы
B) для постоянного хранения обрабатываемых данных
C) для кратковременного хранения обрабатываемых данных и программ
D) для выполнения обработки данных в соответствии с программой
E) все ответы правильные
8.Для запуска программы в системе Windows 98 необходимо:
A) все ответы правильные

B) выбрать в основном меню пункт ПРОГРАММЫ (Programs) и найти необходимую программу
C) щелкнуть на значке документа, связанного с данной программой
D) с помощью ПРОВОДНИКА (Explorer) найти соответствующий программный файл
E) выбрать в контекстном меню пункт СОЗДАТЬ и найти необходимую программу
9.Какая из следующих операций входит в редактирование структуры таблиц:
A) Добавление заданного количества сок;
B) Добавление заданного количества столбцов;
C) Слияние выделенных ячеек;
D) Разбиение выделенных ячеек;
E) Все ответы правильные;
10.Что происходит при нажатии клавиши END?
A) Курсор перемещается в конец текущей страницы
B) Курсор перемещается в конец текущей соки
C) Курсор перемещается в конец текста
D) Происходит закрытие текущего документа
E) Все ответы правильные
11.Как нормально завершить работу Windows 98:
A) комбинацией клавиш: Ctrl+Alt+Del
B) с помощью пункта Главного меню - Завершение работы
C) клавишей Break или Esc
D) с помощью пункта Главного меню - STOP
E) комбинацией клавиш: Ctrl+Shift+Del
12.Какая из программ является графическим редактором
A) Microsoft Word
B) CorelDraw
C) Corel Venture
D) DoctorWeb
E) Far
13.Команды меню ОКНО позволяют управлять:
A) окнами запущенных приложений WINDOWS.
B) окнами запросов.
C) диалоговыми окнами .
D) окнами открытых документов.
E) «Среди предъявленных ответов нет правильного.»
14.Чтобы записать документ (TEXT.DOC) на дискету, надо выбрать из меню «Файл» следующий пункт:
A) Переписать
B) Сохранить как...
C) Сохранить
D) Записать...
E)Среди предъявленных ответов нет правильного

15.В MS Word укажите какая команда меню 'Сервис' позволяет поместить нужные кнопки на панель управления:
A) Настройка
B) Параметры
C) Автозамена
D) Макрос
E) Исправления
16.Какой фирмой была разработана система Windows?
A) Sun Microsistem
B) Microsoft
C) Apple
D) MacCой
E) Borland
17.Основные устройства компьютера: основная память, внешняя(дисковая) память, устройства ввода/вывода. Добав0ьте еще одно устройство:
A) процессор
B) ксерокс
C) факсимильное устройство
D) трансивер
E) сканер
18.Создать новый документ:
A) ФАЙЛ, ОТКРЫТЬ
B) ФАЙЛ, СОЗДАТЬ
C) ВИД, ОБЫЧНЫЙ
D) ОКНО, НОВОЕ
E) Нет правильного ответа
19Какое устройство служит для подключения к сети Интернет?
A) Сканер
B) Дисковод
C) Модем
D) Принтер
E) Системный блок
20 Что происходит при нажатии клавиши HOME?
A) Курсор перемещается в начало текущей соки
B) Курсор перемещается в начало текущей страницы
C) Курсор перемещается в начало текста
D) Происходит загрузка нового документа
E) Все ответы правильные

| Номер вопроса | Правильный ответ | Номер вопроса | Правильный ответ |
|---|---|---|---|
| 1 | B | 11 | B |
| 2 | C | 12 | B |
| 3 | C | 13 | Д |
| 4 | B | 14 | B |
| 5 | B | 15 | A |
| 6 | C | 16 | B |
| 7 | Д | 17 | A |
| 8 | B | 18 | B |
| 9 | E | 19 | C |
| 10 | B | 20 | A |

Программу составил: Уразаков Р.Р.

Программа одобрена на заседании кафедры от _____г., протокол №__

1. *www.informika.ru* – сайт Государственного научно-исследовательского института информационных технологий и теле-коммуникаций (ФГУ ГНИИ ИТТ "Информика")

2. *www.intel.ru* и *www.intel.com* – корпорация Intel

3. *www.microsoft.ru* и *www.microsoft.com* – корпорация Microsoft

4. *pcnews.ru, computer-news.ru , www.hardvision.ru, news.ferra.ru, www.ixbit.com, www.computerra.ru, www.compulenta.ru, www.comp-life.ru* – компьютерные новости

5. *www.itnews.ru, http://subscribe.ru/catalog/comp, www.studioit.ru, www.it-top.ru, www.cnews.ru, it-technologiess.ru, www.worldnewsit.ru* – новости информационных технологий

6. *www.3dnews.ru* – Daily Digital Digest, все о компьютерах – обзоры, аналитика, новости Hardware, новости Software, сети, программное обеспечение, энциклопедия и пр., тематические рассылки

7. *www.intuit.ru* – Интернет-Университет Информационных Технологий, бесплатные курсы (более 400), обучение, видеокурсы и пр.

8. *www.planet-it.ru* – портал предназначен для аккумулирования различ-ных образовательных мероприятий в области информационных тех-нологий: олимпиад, конкурсов, тестов, удаленного обучения и т.д.

9. *www.citforum.ru* – новости, рассылки и форумы по темам: IT-консалтинг, Software Engineering, программирование, СУБД, безопас-ность, Internet, сети, операционные системы, Hardware

10. *www.ict.edu.ru* – информационно-коммуникационные технологии в образовании

11. *www.forum.softweb.ru* – форум с разделами «Компьютер для начи-нающих», «Программы», «Программирование», «Интернет и сети», «Я и компьютер», группы разделов «Образование и работа», библио-тека с книгами для скачивания и пр.

12. *http://forum.oszone.net* – форум с различными группами тем в области информационных технологий

13. *www.cyberforum.ru* – форум программистов

14. *http://vbsbook.ru* – справочник по языку программирования

## 5.3. СРЕДСТВА ОБЕСПЕЧЕНИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

Единое окно доступа к образовательным ресурсам. http://window.edu.ru/

## 6. МАТЕРИАЛЬНО–ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.

Оборудованные аудитории; мультимедийное оборудование, интерактивная доска.

## 7. СОДЕРЖАНИЕ ИТОГОВОГО И ПРОМЕЖУТОЧНОГО КОНТРОЛЯ

### ГРАФИК
### промежуточного и итогового контроля

| № п.п. | Вид контроля (выполнение лабораторных работ, тестирование.) | Сроки проведения | Перечень проверяемых дидактических единиц и компетенций |
|---|---|---|---|
| 1. | Знание терминов и понятий. | | ОК, ПК |
| 2 | Выполнение лабораторных работ. | | ОК, ПК |
| | **Зачет** | | **ОК, ПК** |

### ПЛАН-ГРАФИК СРС

| № п.п. | Разделы (темы) курса | Задание на СРС |
|---|---|---|
| 2. | 1-5 | Работа с материалами лекций, семинаров; дополнительной литературой; терминами, понятиями, персоналиями. |
| 3. | 1-5 | Работа с обработкой информации. Выполнение лабораторных работ. |

### ОСНОВНЫЕ ВИДЫ ЗАНЯТИЙ И ОСОБЕННОСТИ ИХ ПРОВЕДЕНИЯ.

Основной формой ознакомления студентов с теоретическими и методологическими основами религиоведческого знания служат лекционные занятия. Главный акцент на лекциях делается на разъяснении наиболее сложных тем в истории религиоведения и теоретической ее части. Вместе с тем, поднимаются и проблемные, дискуссионные темы, требующие рассмотрения разнообразных подходов.

Задачей практических занятий является усвоение студентами содержания лекционных тем и углубление практических навыков работы с информацией. Основной вид практических занятий – лабораторные работы.

Лабораторные работы носят избирательный характер, проводятся по отдельным темам курса. К целям лабораторных занятий относятся активизация работы студентов в течение всего учебного процесса, формирование навыков самостоятельного поиска и анализа информации, умение аргументировано излагать и отстаивать свое мнение, участвуя в дискуссии, овладение практическими навыками информационного обеспечения и владения информацией у студентов. Одной из задач семинара является организация обсуждения поставленных вопросов с вовлечением всей аудитории. Самостоятельная работа студентов носит обязательный характер и предполагает выполнение лабораторных заданий.

Осуществляется эта работа также с помощью и учетом рекомендаций преподавателя.

## 7.2. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ.

1.Дайте определение термину «информация». Каким образом измеряют информацию? Какие меры информации вам известны?
2.Как связаны между собой количество информации и мера неопределенности состояния системы?
3.Что такое «прагматическая мера информации»? Какими понятиями определяется качество информации?
4.Что такое «кодирование» и «декодирование»?
5.Что такое «классификация»? Что такое «реквизит», «классификатор»?
6. Какие системы кодирования информации применяются при классификации?
7.Расскажите об информационных революциях в истории развития цивилизации.
8.Дйте определение информационной культуре? Как она проявляется?
9. Чем определяется информационный потенциал общества?
10. Расскажите о видах ресурсов? Охарактеризуйте информационный ресурс, информационный продукт, информационную услугу. Приведите примеры?
11.Расскажите о классификации основных видов информационных услуг? Каковы составляющие рынка информационных услуг и продуктов?
12. В чем заключается правовое регулирование на информационном рынке?
13. Как вы понимаете термин «управление знаниями»?
14. Какие процессы включаются в управление знаниями?
15.Какие способы классификации знаний вы знаете?
16.Перечислите признаки интеллектуального поведения?
17. Что может быть источником данных в процессе добычи данных?
18. Что такое «получение знаний»? Какую роль этот процесс играет в инженерии знаний?
19.В чем различие инженерии знаний и управления знаниями?
20.Как вы понимаете информационную технологию?
21.Как развивались информационные системы?
22. В чем сходство и в чем различие информационной технологии и технологии материального производства?

23.Отобразите информационную технологию в виде иерархической структуры и приведите примеры ее составляющих.
24.Что такое инструментарий информационной технологии»? Как соотносятся информационная технология и информационная система?
25. Охарактеризуйте методологию использования информационной технологии.
26.Дайте общее представление об информационных технологиях обработки данных управления, автоматизации офиса, поддержки принятия решений. Назовите их основные компоненты.
27. Расскажите о компьютерных и некомпьютерных офисных технологиях.
28.Дате определение информационной безопасности.
29.Чем определяется информационная безопасность?
30. Каковы основные принципы государственной политики обеспечения информационной безопасности России?
31. Перечислите виды угроз в информационной сфере.
32. Что относится к внутренним и внешним источникам угроз информационной безопасности?
33.Дайте определение организационно-правовому обеспечению информационной безопасности. Что такое государственная тайна?
34. Какие виды ущерба может нанести нарушение Информационной безопасности?
35. Какие вы знаете угрозы информационным системам?
36. В чем заключается нарушение достоверности? Приведите пример.
37. В чем заключается нарушение конфиденциальности? Приведите пример.
38. В чем заключается нарушение целостности? Приведите пример.
39. в чем заключается нарушение доступности? Приведите пример.
40. Каким образом можно классифицировать угрозы информации? Какие способы защиты информации вам известны?

**Программу составил:** _____

Программа одобрена на заседании кафедры от _____г., протокол №__