**ГОУВПО**

**«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**ФАКУЛЬТЕТ ИНЖЕНЕРНОЙ МЕХАНИКИ И МАШИНОСТРОЕНИЯ**

**Кафедра «Управление качеством»**

1. **Конспект лекций**
2. **по нормативной дисциплине цикла профессионально-практической подготовки бакалавров по направлению**
3. **27.03.02 «Управление качеством»**
4. **по дисциплине**
5. **Информационные технологии в управлении качеством и защита информации**

**Донецк – 2016г.**

**ГОУВПО**

**«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**ФАКУЛЬТЕТ ИНЖЕНЕРНОЙ МЕХАНИКИ И МАШИНОСТРОЕНИЯ**

**Кафедра «Управление качеством»**

1. **Конспект лекций**
2. **по нормативной дисциплине цикла профессионально-практической подготовки бакалавров по направлению**
3. **27.03.02 «Управление качеством»**
4. **по дисциплине**
5. **Информационные технологии в управлении качеством и защита информации**

Рассмотрено

На заседании кафедры
«Управление качеством»

Протокол № 2 от «14» «сентября» 2016г.

Утверждено на заседании

Научно-издательского

Совета ДонНТУ

Протокол № \_\_\_ от «\_\_\_» «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_» 20\_\_г.

 Донецьк, 2016 г.

## УДК 658.532

Конспект лекций по курсу «Информационные технологии в управлении качеством и защита информации» для студентов специальности 27.03.02 «Управление качеством» дневной формы обучения. Сост: Масюк Л.Н., Бабенко Г.С. Донецк: ДонНТУ, 2016 г. – 123 с.

В настоящем конспекте лекций изложена теоретическая часть курса по дисциплине «Информационные технологии в управлении качеством и защита информации» в соответствии с рабочей программой курса. Приведен перечень ссылок для успешного усвоения изучаемой дисциплины.

Разработали: Масюк Л.Н., Бабенко Г.С.

**СОДЕРЖАНИЕ**

Введение

Тема 1 Информация и информационные технологии

Тема 2. Управление качеством и информационные технологии.

Тема 3. Информационные системы и информационные технологии в управлении качеством

Тема 4. Экспертные системы в управлении качеством

Тема 5 Современные системы для бизнеса

Тема 6 Корпоративные информационные системы

Тема 7 Актуальность защиты информации.

Тема 8. Источники, риски и формы атак на компьютерную информацию.

Тема 9. Методы защиты информации.

Тема 10. Международные стандарты на системы управления информационной безопасностью.

Заключение

Литература

# ВВЕДЕНИЕ

## Дисциплина рассматривает вопросы: теоретических основ информационных систем в промышленности и экономике, использовании современных технологий и методов обработки информации; интеллектуальные технологии и их применение в экономических системах; аспекты информационной безопасности, а также средств защиты информации.

## Целью дисциплины является: развитие теоретических знаний и практических навыков в области защиты компьютерной информации. Изучении методологии структурного моделирования и улучшения реинжиниринга бизнес процессов с помощью программных средств; формирование теоретических знаний в области правовых и организационных основ защиты информации, средств и методов защиты информации, построения и организации функционирования систем защиты информации в компьютерных системах, методов несанкционированного доступа и взлома; формирование теоретических знаний в области методологии структурного моделирования; освоение приемов реализации известных криптоалгоритмов и алгоритмов сокрытия информации, защиты системного программного обеспечения; изучение вопросов политики безопасности; стандартов безопасности России и развитых стран; тенденций и перспектив развития средств защиты информации.

## Применение настоящего лекционного материала в процессе изучения данной дисциплины способствует не только усвоению теоретического материала курса, но и развитию практических навыков обучающихся через выполнение тренировочных заданий, тестов, контрольных работ, самостоятельную работу с литературой.

## В результате освоения дисциплины студент должен:

## знать: методику применения информационных технологий в управлении качеством, содержание основных понятий защиты информации, источники угроз безопасности, методы пресечения разглашения конфиденциальной информации.

 уметь: применять методику проведения экспертизы качества товаров и услуг с использованием информационных систем, отыскивать необходимые нормативно- правовые акты в системе действующего законодательства; разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.

 Перечисленные результаты обучения являются основой для формирования следующих компетенций: использовать основы экономических знаний в различных сферах деятельности (ОК-3); решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением математического аппарата для осуществления профессиональной деятельности, информационно-коммуникационных технологий, с учетом основных требований информационной безопасности (ОПК-3); использовать основные прикладные программные средства и информационные технологии, применяемые в сфере профессиональной деятельности (ОПК-4); использовать знания о принципах принятия решений в условиях неопределенности и принципах оптимизации на базе внедрения информационных технологий в управление качеством (ПК-6); применять знание принципов и методов разработки и правил применения нормативно-технической документации по обеспечению качества процессов, продукции и услуг, соответствующей установленным нормам, для анализа и решения проблем, используя информационные технологии и системы автоматизированного проектирования (ПК-20).

**Тема 1. ИНФОРМАЦИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**

**1.1 Понятие информационной технологии**

Термин «технология» широко употреблялся до недавнего времени только при изучении производственных процессов. Рассмотрим некоторые определения.

 «Технология (от греческого - искусство, мастерство, умение и ...логия) - совокупность методов обработки, изготовления, изменения состояния, свойств, формы сырья, материала или полуфабриката, осуществляемых в процессе производства продукции»Советский энциклопедический словарь. - М., 1979. - С. 1338.

«Технология - совокупность производственных методов и процессов отрасли производства, а также научное описание способов производства...»Ожегов С.И. Толковый словарь русского языка / С.И. Ожегов, Н.Ю. Шведова. – М.: ООО «ИТИ Технологии», 2003. – С. 797.

«Технология - ...1) совокупность методов обработки, изготовления, изменения состояния, свойств, формы сырья, материала или полуфабриката в профессии производства, например, технология металлов, химическая технология, технология строительных работ; 2) наука о способах воздействия на сырье, материалы или полуфабрикаты соответствующими орудиями производств» [Политический словарь. - М., 1989. - С. 534].

Очевидно, что технология - это научное решения практических задач, а расцвет современных технологий напрямую можно связать с научно-технической революцией.

Все приведенные определения ориентированы по производственно-промышленному «вектору». Однако, понятие «технология» со временем содержательно оказалось намного богаче. Потенциальные возможности понятия «технология» в ходе его использования в традиционной сфере постоянно возрастали. Область, в пределах которой это понятие употреблялось, стала интенсивно расширяться, и вследствие этого, включать в себя педагогику, социологию, культуру и т.д.

Таким образом, сегодня понятие «технология» можно рассматривать на разных уровнях. На философском уровне технология– учение о наилучшей (оптимальной) деятельности. На межпредметном уровне это процесс, определяемый совокупностью средств иметодов обработки, изготовления, изменения состояния, свойств, формысырьяили материала. Наконец, на общеобразовательном уровне технологию определяют как область знаний, методов и средств, используемых для оптимального преобразования и применения материи (материалов), энергии и информации по плану и в интересах человека, общества, окружающей среды.

Замена материального объекта на идеальный (информацию) позволяет использовать понятие технологии в области, касающейся обработки и производства информации с применением современных средств компьютерной техники.

Информация является одним из ценнейших ресурсов общества нарядус такими традиционными материальными видами ресурсов как нефть, газ, полезные ископаемые и др. Понятие «информация» вышло на передний край науки сравнительно недавно. В старых словарях его не найти. Первые научные труды, составившие фундамент теории информации, появились примерно семьдесят лет назад. И чуть более пятидесяти лет назад академик А.Н. Колмогоров отнес информацию к важнейшим научным понятиям и назвал ее первоосновой новых перспективных отраслей науки и техники.

В условиях современного рынка актуальным становится определение информации, которое дает В.Л. Тамбовцев: «Информация – это те продукты или услуги, которые предназначены их производителем для передачи знаний в максимально доступной для потенциального потребителя форме» [12, с. 10].

Понятие информации – это и более широкое, и в каком-то смысле более узкое понятие, чем знание. Общий поток информации, который поступает из внешнего мира в мозг человека через его органы чувств, выражается числом 100 000 битов в секунду. Но лишь тысячная доля этой информационной лавины становится фактом сознания. На своем высшем уровне отражение в своей результативной форме выступает как знание. Зададимся вопросом – можно ли знание отождествлять с информацией? Как пишет А.Г. Спиркин: «...Знание противоположно незнанию, т.е. отсутствию проверенной информации о чем-либо...» [11]. Знания могут появиться только после получения и переработки информации. Таким образом, знание выступает звеном в цепи: возникновение - передача - получение - переработка - дальнейшая передача трансформированной информации.

Конечно, понятия «информация» и «знание» очень близки, а знание, осведомленность играют сегодня очень важную роль в жизни людей. Для технической науки, как информатика, понятие информации, однако, не может основываться на таких антропоцентрических понятиях, как знание, и не может опираться только на объективность фактов и свидетельств. Об этом пишет С.В.Симонович [7, с. 13]: «Средства вычислительной техники обладают способностью обрабатывать информацию автоматически, без участия человека, и ни о каком знании или незнанииздесь речь идти не может. Эти средства могут работать с искусственной, абстрактной и даже с ложной информацией, не имеющей объективного отражения ни в природе, ни в обществе». В своей книге он дает следующее определение информации: «Информация – это продукт взаимодействия данных и адекватных им методов».

Приведем еще одно определение информации: «Информатика рассматривает информацию как концептуально связанные между собой сведения, данные, понятия, изменяющие наши представления о явлении или объекте окружающего мира» [8, с. 41]. Кроме понятия «информация» в информатике часто используется понятие «данные». Данные могут рассматриваться как признаки или записанные наблюдения, которые по каким-то причинам не используются, а только хранятся. Если данные участвуют в процессе снятия неопределенности, то данные становятся информацией. Следовательно, можно утверждать, что информацией являются используемые данные.

Итак, для различных областей науки существуют свои определения понятия «информация».

Идея включения информации в цепочку производства информационного продукта принадлежит В.М. Глушкову. В 1982 году в своей книге «Основы безбумажной информатики» он дал следующее определение: «Информационные технологии – процессы, где основной перерабатываемой продукцией является информация» [6, с. 334]. Отсюда вытекает положение о том, что информационные технологии использовались всегда, так как задачи накопления, обработки и распространения информации стояли перед человечеством на всех этапах его развития. Особенно широко информационные технологии применялись для обучения.

Почему же об информационных технологиях заговорили не так давно? Н.В. Апатова отмечает, что «методические системы не называли информационными технологиями потому, что данный термин связан с появлением вычислительной техники» [2, с. 6]. По мнению Н.В. Апатовой, информационная технология – это некая методическая система, то есть часть педагогической технологии.

В некоторых работах мы встречаемся с такими определениями информационных технологий обучения, которые не дают полного представления обо всех областях их применения. В частности, Н.В. Апатова пишет: «Информационная технология обучения – процесс подготовки и передачи информации обучаемому, средством осуществления которого является компьютер» [2, с. 7]. Здесь правильнее было бы говорить о компьютерных, а не об информационных технологиях обучения, так как понятие информационных технологий гораздо шире.

В [5, с. 20] дается следующее определение: «Информационная технология – комплекс методов, способов и средств, обеспечивающих хранение, обработку, передачу и отображение информации и ориентированных на повышение эффективности и производительности труда».

Под *информационными технологиями* в широком смысле будем понимать совокупность средств и методов сбора, обработки и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса или явления (информационного продукта) [3, с. 87].

Существенным отличием информационных технологий от других областей науки и производства является то, что они претерпевают постоянные изменения, вызванные бурным развитием средств компьютерной техники и современной связи. Сегодня говорят не просто об информационных технологиях, а о современных или новых информационных технологиях (НИТ). Их основу, по мнению А.Н. Богатырева, А.В. Коптелова и Г.Н. Некрасовой, составляют пять технических достижений [4, с. 5]:

1. Появление новой среды накопления информации на машиночитаемых носителях.
2. Развитие средств связи, обеспечивающих доставку информации практически в любую точку земного шара без существенных ограничений во времени и расстоянии, широкий охват населения средствами связи.
3. Динамичное развитие микропроцессорной техники, обеспечивающей возможность цифровой обработки информации.
4. Возможность автоматизированной обработки информации с помощью компьютера по заданным алгоритмам.
5. Возникновение и бурное развитие сети Интернет.

Итак, новыми информационными технологиями обучения будем называть совокупность электронных средств и способов их функционирования, используемых для реализации обучающей деятельности. Технологии, которые существовали до появления вычислительной, микропроцессорной техники, будем называть традиционными информационными технологиями. Они по-прежнему успешно применяются в образовании и вряд ли будут полностью вытеснены новыми информационными технологиями.

Что же является целью информационной технологии? В [3, с. 344] находим: «Цель информационной технологии – производство информации, удовлетворяющей информационные потребности человека. Чаще всего эти потребности связаны с принятием решений в таких сферах, как познание, общение, практическая (производственная) деятельность». В этой же работе отмечается, что отличительной особенностью технологии является то, что применение одной и той же технологии к одинаковому исходному «сырью» дает в результате «продукт» одного и того же качества. С другой стороны, применяя разные технологии к одному и тому же ресурсу, можно получить разные продукты.

Подобно тому, как в материальной технологии выделяются ее составляющие (материаловедение, проектирование, производственные процессы, инструментарий, техника безопасности и охрана труда, теория управления предприятием), так и информационную технологию можно разделить на части: теория информации, моделирование и формализация, информационные процессы, информационные системы, информационная безопасность и информационное управление.

Информационная технология, как и любая другая, должна отвечать следующим требованиям:

* обеспечивать высокую степень разделения всего процесса обработки информации на этапы, операции, действия;
* включать весь набор элементов, необходимых для достижения поставленной цели;
* иметь регулярный характер. Этапы, действия, операции технологического процесса могут быть стандартизированы и унифицированы, что позволит более эффективно осуществлять целенаправленное управление информационными процессами.

На сегодняшний день существуют различные подходы к проблеме классификации информационных технологий. Приведем несколько классификаций. В [8] выделяются следующие виды информационных технологий:

* информационная технология обработки данных,
* информационная технология управления,
* автоматизация офиса,
* информационная технология поддержки принятия решений,
* информационная технология экспертных систем.

В [13, с. 17] информационные технологии подразделяют на различные виды следующим образом:

* функционально-ориентированные информационные технологии, предназначенные для реализации определенных задач,
* предметно-ориентированные информационные технологии, предназначенные для решения конкретных задач в определенной предметной области,
* проблемно-ориентированные информационные технологии, предназначенные для решения типовых прикладных задач.

Мы будем придерживаться классификации, приведенной авторами учебника [3], которая составлена в зависимости от формы представления обрабатываемой информации:

* технологии обработки текстовой информации,
* технологии обработки числовой информации,
* технологии обработки графической информации,
* технологии обработки звуковой информации,
* технологии работы в глобальных сетях,
* социальные информационные технологии.

Выбор данной классификации объясняется тем, что сложилась традиция обучать школьников и студентов именно этим видам информационных технологий.

## 1.2 Информатизация общества

В истории человеческого общества несколько раз происходили радикальные изменения и в информационной области, которые можно назвать информационными революциями.

*Первая информационная революция была связана с изобретением письменности.* Письменность создала возможность накопления и распространения знаний, для передачи знаний будущим поколениям. Цивилизации, освоившие письменность, развивались быстрее других, достигали более высокого культурного и экономического уровня. Примерами могут служить Древний Египет, страны Междуречья, Китай. Позднее переход от пиктографического и идеографического письма к алфавитному, сделавший письменность более доступной, в значительной степени способствовал смещению центров цивилизации в Европу (Греция, Рим).

*Вторая информационная революция (середина XVI в.) была связана с изобретением книгопечатания.* Стало возможным не только сохранять информацию, но и сделать ее массово-доступной. Грамотность становится массовым явлением. Все это ускорило рост науки и техники, помогло промышленной революции. Книги перешагнули границы стран, что способствовало началу создания общечеловеческой цивилизации.

*Третья информационная революция (конец XIX в.) была обусловлена прогрессом средств связи.* Телеграф, телефон, радио позволили оперативно передавать информацию на любые расстояния. Эта революция не случайно совпала с периодом бурного развития естествознания.

*Четвертая информационная революция (70-е гг. XX в.) связана с появлением микропроцессорной техники и, в частности, персональных компьютеров.* Вскоре после этого возникли компьютерные телекоммуникации, радикально изменившие системы хранения и поиска информации. Были заложены основы преодоления информационного кризиса.

Четвертая информационная революция дала толчок к столь существенным переменам в развитии общества, что для его характеристики появился новый термин «информационное общество».

Само название впервые возникло в Японии. Специалисты, предложившие этот термин, разъяснили, что он определяет общество, в котором в изобилии циркулирует высокая по качеству информация, а также есть все необходимые средства для ее хранения, распределения и использования. Информация легко и быстро распространяется по требованиям заинтересованных людей и организаций и выдается им в привычной для них форме. Стоимость пользования информационными услугами настолько невысока, что они доступны каждому.

Академик В.А. Извозчиков предлагает следующее определение: «Будем понимать под термином «информационное» («компьютеризированное») общество то, во все сферы жизни и деятельности членов которого включены компьютер, телематика, другие средства информатики в качестве орудий интеллектуального труда, открывающих широкий доступ к сокровищам библиотек, позволяющих с огромной скоростью производить вычисления и перерабатывать любую информацию, моделировать реальные и прогнозируемые события, процессы, явления, управлять производством, автоматизировать обучение и т. д.» [9, с. 107]. Здесь термин «телематика» означает обработку информации на расстоянии.

Проследим более детально существующие тенденции в развитии информационного общества. Однако вначале отметим, что в настоящее время ни одно государство не находится в этой стадии. Ближе всех к информационному обществу подошли США, Япония, ряд стран Западной Европы.

Не существует общепринятого критерия оценки полномасштабного информационного общества, однако известны его формулировки. Интересный критерий предложил академик А.П. Ершов: «О фазах продвижения к информационному обществу следует судить по совокупным пропускным способностям каналов связи» [9, с. 108]. За этим стоит простая мысль: развитие каналов связи отражает и уровень компьютеризации, и объективную потребность общества во всех видах информационного обмена, и другие проявления информатизации. Согласно этому критерию, ранняя стадия информатизации общества наступает при достижении действующей в нем совокупной пропускной способности каналов связи, обеспечивающей развертывание достаточно надежной междугородной телефонной сети. Завершающая фаза – при возможности реализации надежного и оперативного информационного контакта между членами общества по принципу «каждый с каждым». На завершающей фазе пропускная способность каналов связи должна быть в миллион раз больше, чем в первой фазе.

Следует обратить внимание на то, что сегодня все больше людей в обществе заняты работой с информацией. Информация позволяет человеку познавать мир, ощущать себя его частью, общаться с другими людьми, воспитывать детей, решать бытовые проблемы, заниматься различного рода деятельностью, творческим трудом. С помощью информации организуется совместный труд людей на предприятиях, образуются их профессиональные союзы и общества. Информация является основой деятельности органов законодательной, исполнительной и судебной власти, системы государственного управления.

*Информационное общество* – общество, в котором большинство работающих занято производством, хранением, переработкой и реализацией информации, особенно высшей ее формой – знаний. Движущей силой развития общества должно стать производство не материального, а информационного продукта. Материальный продукт станет более информационно емким, что означает увеличение доли инноваций, дизайна и маркетинга в его стоимости.

Согласно мнению ряда специалистов, США завершат в целом переход к информационному обществу к 2020 году, Япония и большинство стран Западной Европы к 2030-2040 годам.

Переход к информационному обществу сопровождается переносом центра тяжести в экономике с производства материальных благ (товаров) на оказание услуг, что влечет за собой значительное снижение добычи и переработки сырья и расхода энергии.

Вторая половина XX века, благодаря информатизации, сопровождалась перетоком людей из сферы прямого материального производства в информационную сферу. Промышленные рабочие, составлявшие в середине XX века более 2/3 населения, сегодня в развитых странах составляют менее 1/3. Значительно разросся социальный слой, который называют «белые воротнички» – люди наемного труда, не производящие непосредственно материальных ценностей, а занятые обработкой информации (в широком смысле): учителя, банковские служащие, программисты и т. д. Так, к 1980 году в сельском хозяйстве было занято 3% работающих, в промышленности – 20%, в сфере обслуживания – 30%, и 47% людей было занято в информационной сфере [9, с. 108].

Самое главное, информатизация изменила и характер труда в традиционных отраслях промышленности. Появление робототехнических систем, повсеместное внедрение элементов микропроцессорной техники является основной причиной этого явления.

Приведем пример: в станкостроительной отрасли в США в 1990 году было занято 330 тыс. человек, а к 2005 году осталось 14 тыс. человек. Это произойдет за счет массового сокращения людей на сборочных линиях, вследствие внедрения вместо них роботов и манипуляторов.

Еще одна характерная черта в этой сфере – появление развитого рынка информационных продуктов и услуг. Этот рынок включает секторы:

* деловой информации (биржевая, финансовая, статистическая, коммерческая информация);
* профессиональной информации (научно-техническая информация, первоисточники и пр.);
* потребительской информации (новости, всевозможные расписания, развлекательная информация);
* услуг образования и другие.

Однако есть и негативная сторона процесса информатизации, суть которой заключается в том, что поток информации, хлынувший на человека, столь велик, что недоступен обработке в приемлемое время. Это так называемый *информационный кризис.*

Это явление имеет место и в научных исследованиях, и в технических разработках, и в общественно-политической жизни. В нашем усложняющемся мире принятие решений становится все более ответственным делом, а оно невозможно без полноты информации.

Ускорение накопления общего объема знаний происходит с удивительной быстротой. В начале XX века общий объем всей производимой человечеством информации удваивался каждые 50 лет, к 1950 году удвоение происходило каждые 10 лет, к 1970 году – уже каждые 5 лет; конца этому процессу ускорения пока не видно.

Информационный кризис проявляется в следующем:

* информационный поток превосходит ограниченные возможности человека по восприятию и переработке информации;
* возникает большое количество избыточной информации (так называемый «информационный шум»), которая затрудняет восприятие полезной для потребителя информации;
* возникают экономические, политические и другие барьеры, которые препятствуют распространению информации (например, по причине секретности).

Частичный выход из информационного кризиса видится в применении новых информационных технологий. Внедрение современных средств и методов хранения, обработки и передачи информации многократно снижают барьер доступа к ней и скорость поиска. Разумеется, одни лишь технологии не могут решить проблему, имеющую и экономический характер (информация стоит денег), и юридический (информация имеет собственника), и ряд других. Эта проблема комплексная и решается усилиями как каждой страны, так и мирового сообщества в целом.

В основе информационной революции лежит взрывное развитие информационных и коммуникационных технологий. В этом процессе отчетливо наблюдается и обратная связь: движение к информационному обществу резко ускоряет процессы развития указанных технологий, делая их широко востребованными.

Однако сам по себе бурный рост производства средств вычислительной техники, начавшийся с середины XX века, не стал причиной перехода к информационному обществу. Компьютеры использовались сравнительно небольшим числом специалистов до тех пор, пока существовали обособленно. Важнейшим этапом на пути в информационное общество стало:

* создание телекоммуникационной инфраструктуры, включающей в себя сети передачи данных;
* появление огромных баз данных, доступ к которым через сети получили миллионы людей;
* выработка единых правил поведения в сетях и поиск в них информации.

Огромную роль в обсуждаемом процессе сыграло создание международной компьютерной сети Интернет. Сегодня она представляет собой колоссальную и быстро (на 10-15% в месяц) растущую систему, число пользователей которой перевалило за 200 миллионов человек.

Необходимо отметить, что в настоящее время в мире наблюдается отказ от создания собственных корпоративных сетей в пользу открытых стандартизованных систем и их интеграции в Интернет (за исключением, конечно, сетей специального назначения, в которых очень высоки требования к безопасности информации).

Информационные и коммуникационные технологии постоянно развиваются. Постепенно происходит универсализация ведущих технологий, то есть вместо создания для решения каждой задачи собственной технологии разрабатываются мощные универсальные технологии, допускающие много вариантов использования. Хорошо знакомый пример – офисные системы программного обеспечения, в которых можно производить множество разнообразных действий, от простейшего набора текста до создания специальных программ (например, начисления заработной платы с помощью табличного процессора).

Универсализации информационных технологий способствует широкое использованием мультимедиа. Современная мультимедийная система способна объединить функции, например, компьютера, телевизора, радиоприемника, телефона, автоответчика, факса, обеспечивая при этом и доступ к сетям передачи данных.

Существование вычислительной техники приводит к персонализации и миниатюризации устройств хранения информации. Крошечные, умещающиеся на ладони устройства, имеющие все функции персонального компьютера, позволяют человеку обзавестись собственным универсальным справочником, объем информации в котором сопоставим с несколькими энциклопедиями. Поскольку это устройство может быть подключено к сети, то оно же передает и оперативные данные, например: о погоде, текущем времени, состоянии пробок на дорогах и т. д.

Рассмотрим понятие «информационная культура». Понятие информационной культуры личности в настоящее время окончательно не определено и трактуется по-разному. Наиболее часто оно употребляется для обозначения широты знаний специалиста.

Разнообразие взглядов, характеризующих отдельные стороны информационной культуры специалиста, таким образом, сводится по крайней мере к трем позициям. В качестве предмета при ее анализе все авторы исследуют знания, которыми должен владеть специалист. Это-первое, что объединяет их при обсуждении данной проблемы. Второе связано с тем, что информационная культура обозначается как качественная характеристика личности. Третье – она отражает уровень информатизации общества.

Современный этап перехода человечества, от «индустриального общества» к «информационному» выдвигает ряд требований к деятельности субъекта, которые дают основание говорить о некоторых общих подходах к формированию информационной культуры участников образовательного процесса. Человеку информационного общества необходимы такие знания и навыки, которые, с одной стороны, энергично и эффективно можно использовать для дальнейшего продвижения науки, техники, культуры, для выявления огромного потенциала компьютерных технологий, а, с другой стороны, эти знания и навыки должны стать гарантом суверенизации личности ради наиболее полной реализации созидательных ресурсов человека.

Анализ теоретических источников показывает, что некоторые грани информационной культуры человека в достаточной степени определены. Сформулированы требования к специалисту – выпускнику педагогического института; рассмотрены отдельные стороны информационной культуры; выявлены специфические черты современных процессов, происходящих в обществе. Информационная культура является составной частью педагогической культуры. Важнейшей составляющей информационной культуры в современных условиях, в свою очередь, является компьютерная культура участника образовательного процесса.

К общей компьютерной культуре целесообразно отнести навыки использования компьютерной техники и эрудицию в области созданных для этого профессиональных прикладных программ. К специальной компьютерной культуре – знания, обеспечивающие возможность специалисту работать на стыке своей профессии с информатикой и вычислительной техникой. Она развивается на понимании основных идей информатики и представлений о роли информационных и телекоммуникационных технологий в жизни общества и в профессиональной деятельности специалиста, а также общих навыков использования компьютерной техники, умения использовать компьютеризированные информационные и телекоммуникационные технологии.

Для 96% участников образовательного процесса компьютерная культура предполагает наличие знаний, обеспечивающих возможность преподавателю и студенту пользоваться при обучении основными понятиями информатики, вычислительной техники, а также владение навыками решения задач профессиональной деятельности с использованием компьютеров, эрудицию в области созданных для этого специальных прикладных программ [10, с. 86].

Совершенствование компьютерной культуры – настоятельное веление времени, непременное требование к современному специалисту. Для решения этой проблемы во всех учебных заведениях, необходимо формировать новое мышление, опирающееся на осознание безусловной необходимости использования и применения в любом виде профессиональной деятельности педагога современной компьютерной техники, информационных и телекоммуникационных технологий, овладение которыми возможно лишь на базе компьютерной грамотности.

Успешная реализация задач постепенного, но постоянного повышения уровня компьютерной грамотности всех участников процесса обучения в педагогическом институте обеспечивается следующими условиями:

* изучением студентами предметов информационного цикла, дающих обучаемым знания, умения и навыки, достаточные знания правильного понимания значения информации и эффективной работы с технологиями целенаправленной деятельности, функционирующими на основе производства различных операций с профессионально значимой информацией (информационными технологиями);
* созданием благоприятных условий заинтересованности преподавательского состава в повышении уровня своей компьютерной подготовки.

Данная цель связана не столько с формированием необходимого уровня компьютерной грамотности, сколько, наряду с ним, с изучением и усвоением обучаемыми особенностей и возможностей одного из основных видов проявления человеческого интеллекта – системного мышления. Изучение системного подхода воспитывает особую культуру мышления, и поэтому оно окажется продуктивным в освоении не только математики, информатики, но практически всех дисциплин, предметом изучения которых являются сложные объекты окружающего мира.

Внедрение информационных технологий в образовательный процесс предполагает овладение компьютерной культурой как со стороны объектов, так и со стороны субъектов процесса обучения.

Главным условием здесь является всесторонняя и целенаправленная подготовка к умелому и грамотному использованию информационных технологий преподавательским составом. Именно от их увлеченности современной компьютерной техникой зависит активное внедрение информационных технологий в образовательный процесс вуза, а также успешное обучение основам устройства и применения компьютеров.

## 1.3 Информация, ее представление и измерение

Наверное, самый сложный вопрос в информатике – это «Что такое информация?». Мы уже отмечали, что на него нет однозначного ответа. Такие понятия иногда называют «контекстными», то есть придаваемый им смысл зависит от контекста, в котором они употребляются.

Информация обладает динамическим характером. Она существует только в момент взаимодействия данных и методов. Все остальное время она пребывает в состоянии данных. Таким образом, информация существует только в момент протекания информационного процесса.

Одни и те же данные могут в момент потребления поставлять разную информацию в зависимости от степени адекватности взаимодействующих с ними методов. Например, для учащегося, не владеющего каким-либо языком, текст, написанный на этом языке, дает только ту информацию, которую можно получить методом наблюдения (количество символов, наличие незнакомых символов и т.д.). Использование же более адекватных методов даст иную информацию.

Данные являются объективными, поскольку это результат регистрации объективно существовавших сигналов, вызванных изменениями в материальных телах или полях. В то же время, методы являются субъективными. В основе искусственных методов лежат алгоритмы (упорядоченные последовательности команд), составленные и подготовленные людьми (субъектами). В основе естественных методов лежат биологические свойства субъектов информационного процесса. Таким образом, «информация возникает и существует в момент диалектического взаимодействия объективных данных и субъективных методов» [3, с. 15].

Характерной особенностью информации, отличающей ее от других объектов природы и общества, является то, что на свойства информации влияют свойства данных, составляющих ее содержательную часть, и свойства методов, взаимодействующих с данными в ходе информационногопроцесса. Информация обладает множеством свойств. Каждая научная дисциплина рассматривает те свойства, которые ей наиболее важны. С точки зрения информатики и педагогики наиболее важными представляются следующие свойства: объективность, полнота, достоверность, адекватность, доступность и актуальность информации.

*Объективность* и *субъективность* информации. Понятие объективности является относительным, так как методы являются субъективными. Более объективной принято считать ту информацию, в которую методы вносят меньший субъективный элемент.

*Полнота* информации. Полнота информации во многом характеризует качество информации и определяет достаточность данных для принятия решений или для создания новых данных на основе имеющихся. Чем полнее данные, тем шире диапазон методов, которые можно использовать.

*Достоверность* информации. Данные возникают в момент регистрации сигналов, но не все сигналы являются «полезными» – всегда присутствует какой-то уровень посторонних сигналов, в результате чего полезные данные сопровождаются определенным уровнем «информационного шума». Если полезный сигнал зарегистрирован более четко, чем посторонние сигналы, достоверность информации может быть более высокой.

*Адекватность* информации – это степень соответствия реальному объективному состоянию дела. Неадекватная информация может образовываться при создании новой информации на основе неполных или недостоверных данных. Однако и полные, и достоверные данные могут приводить к созданию неадекватной информации в случае применения к ним неадекватных методов.

*Доступность информации* – мера возможности получить ту или иную информацию. На степень доступности информации влияют одновременно как доступность данных, так и доступность адекватных методов для их интерпретации. Отсутствие доступа к данным или отсутствие адекватных методов обработки данных приводят к одинаковому результату: информация оказывается недоступной.

*Актуальность* информации – это степень соответствия информации текущему моменту времени. Поскольку информационные процессы растянуты во времени, то достоверная и адекватная, но устаревшая информация может приводить к ошибочным решениям.

*Репрезентативность* информации связана с правильностью ее отбора и формирования в целях адекватного отражения свойств объекта. Важное значение здесь имеют:

* правильность концепции, на базе которой сформулировано исходное понятие;
* обоснованность отбора существенных признаков и связей отображаемого явления.

Нарушение репрезентативности информации нередко приводит к существенным ее погрешностям.

*Содержательность* информации отражает семантическую емкость, равную отношению количества семантической информации в сообщении к объему обрабатываемых данных, то есть

 ,

где *Ic*– количество семантической информации,

 *Vд* – объем данных.

*Точность* информации определяется степенью близости получаемой информации к реальному состоянию объекта, процесса, явления и т.п.

*Устойчивость* информации отражает ее способность реагировать на изменения исходных данных без нарушения необходимой точности. Устойчивость информации, как и репрезентативность, обусловлена выбранной методикой ее отбора и формирования.

Приведем классификацию информации, данную С.А. Бешенковым и Е.А. Ракитиной [3, с. 43]:

1. По способу восприятия:
* визуальная,
* аудиальная,
* обонятельная,
* вкусовая,
* тактильная.
1. По степени значимости:
* личная,
* специальная,
* общественная.

Личная – это знания, опыт, интуиция, умения, планы, прогнозы, эмоции, чувства, наследственная память конкретного человека. Специальная делится на научную, производственную, техническую, управленческую. Общественнаявключает в себя общественно-политическую, научно-популярную, обыденную, эстетическую.

1. По форме представления:
* текстовая,
* числовая,
* графическая,
* звуковая.
1. По способам (субъектам) обмена:
* социальная,
* техническая,
* биологическая,
* генетическая.

Приведем другой вариант классификации информации:

* по сфере применения информации (экономическая, географическая, социологическая и пр.);
* по характеру источников информации (первичная, вторичная, обобщающая и пр.);
* по характеру носителя информации (информация, «зашифрованная» в молекулах ДНК или в длинах световых волн, информация на бумажном или магнитном носителе и пр.).

В зависимости от типа носителя различают следующие виды информации [1, с. 51]:

* документальную;
* акустическую (речевую);
* телекоммуникационную.

*Документальная* информация представляется в графическом или буквенно-цифровом виде на бумаге, а также в электронном виде на магнитных и других носителях.

*Речевая* информация возникает в ходе ведения разговоров, а также при работе систем звукоусиления и звуковоспроизведения. Носителем речевой информации являются звуковые колебания в диапазоне частот от 200…300 Гц до 4…6 кГц.

*Телекоммуникационная* информация циркулирует в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче. Носителем информации при ее обработке техническими средствами и передаче по проводным каналам связи является электрический ток, а при передаче по радио- и оптическому каналам – электромагнитные волны.

Источник информации может вырабатывать непрерывное сообщение (сигнал), в этом случае информация называется *непрерывной*, или дискретной – информация называется *дискретной*.

Например, сигналы, передаваемые по радио и телевидению, а также используемые в магнитной записи, имеют форму непрерывных, быстро изменяющихся во времени зависимостей. Такие сигналы называются непрерывными, или *аналоговыми* сигналами. В противоположность этому в телеграфии и вычислительной технике сигналы имеют импульсную форму и называются *дискретными* сигналами.

Сравнивая непрерывную и дискретную формы представления информации, нетрудно заметить, что при использовании непрерывной формы для создания вычислительной машины потребуется меньшее число устройств (каждая величина представляется одним, а не несколькими сигналами), но эти устройства будут сложнее (они должны различать значительно большее число состояний сигнала).

Информация, циркулирующая в обществе, требует специальных средств и методов обработки, хранения и использования. Сформировались новые научные дисциплины – кибернетика, бионика, робототехника и другие, имеющие своей целью изучение закономерностей информационных процессов.

Существует три подхода к измерению информации:

I подход. – Неизмеряемость информации в быту (информация как новизна).

II подход. – Технический или объемный (информация как сообщения в форме знаков или сигналов, хранимые, перерабатываемые и обрабатываемые с помощью технических устройств).

В вычислительной технике применяются две стандартные единицы измерения информации: *бит* и *байт.* Поскольку компьютер предназначен для обработки больших объемов информации, то используют производные единицы – *килобайт* (Кб)*, мегабайт* (Мб), *гигабайт* (Гб). Обычно приставка «кило» означает тысячу, а приставка «мега» - миллион. Но в вычислительной технике осуществляется привязка к принятой двоичной системе кодирования.

В силу этого один килобайт равен не 1000 байтов, а 210 = 1024 байта.

Аналогично, 1 Мб = 210 Кб = 1024 Кб = 220 байтов = 1 048 576 байтов.

1 Гб = 210 Мб = 1024 Мб = 220 Кб = 230 байтов = 1 073 741 824 байта.

III подход. – Вероятностный. Измерение информации в теории информации (информация как снятая неопределенность).

Получение информации (ее увеличение) означает увеличение знания, что, в свою очередь, означает уменьшение незнания или информационной неопределенности.

За единицу количества информации принимают выбор одного из двух равновероятных сообщений («да» или «нет», «1» или «0»). Она также названа *битом.*

**Тема 2 УПРАВЛЕНИЕ КАЧЕСТВОМ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**

1. **Методы управления качеством**.

Качество - емкая, сложная и универсальная категория, имеющая множество особенностей и различных аспектов. В зависимости от цели использования и рассмотрения, можно выделить несколько методов управления качеством.

Методы управления качеством представляют собой способы и приемы осуществления управленческой деятельности и воздействия на управляемые объекты для достижения поставленных целей в области качества. В практике управления качеством используются, в основном, административные, технологические, экономические и психологические методы.

Сущность административного метода управления качеством

Административные методы управления качеством осуществляются посредством обязательных для исполнения директив, приказов и других предписаний, направленных на повышение и обеспечение необходимого уровня качества.

В группу административных методов управления качеством следует включать методы:
- регламентирования (общеорганизационного, функционального, должностного, структурного);
- стандартизации (на основе стандартов различного уровня и статуса);
- нормирования (на базе норм времени, численности, соотносительности, численных величин);
- инструктирования (ознакомления, объяснения, совета, предостережения, разъяснения);
- распорядительных воздействий (на основе приказов, распоряжений, указаний, постановлений, контроля исполнения с использованием превентивного и оперативного воздействий и т. п.);
- приказы и распоряжения по управлению качеством; контроль за исполнением требований и решений по управлению и [обеспечению качества](http://center-yf.ru/data/Menedzheru/obespechenie-kachestva.php);
- логическая последовательность и четкость изложения информации;
- краткость, конкретность, простота и точность формулировок, исключающих возможность неоднозначного толкования;
- убедительность аргументации;
- информационная выразительность;
- достаточность и обоснованность;
- небольшой объем;
- малоизменчивость (стабильность);
- качественная содержательность.

Политика в области качества является одной из важнейших составных частей управления качеством. Данный документ должен быть первичным в составе документации при использовании административных методов управления качеством, это связано с необходимостью принятия ответственности высшим звеном менеджеров за проведение политики в области качества, что в принципе становится первоначальным при реализации системного управления качеством. При формировании политики предприятия в области качества следует учитывать требования, предъявляемые к ней; руководство должно определять политику в письменной форме, она подписывается первым руководителем; она должна согласовываться с другими направлениями деятельности предприятия; руководство должно обеспечивать понимание каждым членом коллектива разработанной политики в области качества, неуклонно ее осуществлять и проводить в жизнь; она должна быть сформулирована таким образом, чтобы ее положения касались каждого члена трудового коллектива, а не только качества выпускаемой продукции. Документ, раскрывающий политику в области качества, должен быть кратким, простым, доходчивым и запоминающимся, отражать требования к качеству работы каждого работника. По существу, приемлемой политикой в области [качества продукции](http://center-yf.ru/data/Menedzheru/Kachestvo-produkcii.php) может быть признана та, которая положительно отвечает на ряд вопросов: является ли она краткой; касается ли она каждого работника коллектива предприятия; установлены ли в ней стандарты (требования) к качеству работы; охвачены ли в ней все аспекты качества поставляемой потребителю продукции и услуг (этот вопрос следует относить также к срокам поставки продукции, иене, качеству конечных результатов деятельности предприятия, включая услуги); подписана ли политика в области качества первым лицом предприятия?

В зарубежной практике политика в области качества формулируется таким образом, что отвечает на многие перечисленные выше вопросы.

Сущность технологического метода управления качеством

По существу все технологические методы можно подразделить на взаимосвязанные между собой способы управления качеством технологических процессов и контроля качества выпускаемой продукции, а также на способы их совокупного использования. Современное состояние науки и техники позволяет осуществлять управление качеством разнообразными инженерно-технологическими методами, и конкретный их выбор во многом зависит от свойств управляемого объекта. Все эти методы управления качеством условно можно классифицировать на автоматические, автоматизированные, механизированные и ручные. Наиболее приемлем для более полного удовлетворения требований потребителей целенаправленный автоматический метод управления качеством. При использовании этого метода отклонения процессов от заданных параметров и соответствующие действия (управляющие меры) определяются, вырабатываются и воздействуют на объект автоматически с помощью технических устройств. Следует отметить, что данный метод является самым перспективным как для управления технологическими процессами, так и особенно для технического контроля качества продукции. В последнем случае применение автоматического метода особенно важно, гак как он не позволяет пропускать ни одного дефектного и бракованного изделия. Использование автоматического технического контроля качества продукции обязывает изготовителя применять неразрушающие методы контроля. Однако в некоторых случаях могут применяться на определенных стадиях производства разрушающие способы контроля.

Наряду с указанными способами в практике управления качеством широко используются также статистические методы.

Они представляют собой взаимосвязанный комплекс методов отслеживания качества на основе статистических данных:

- статистическое регулирование;
- статистический приемочный контроль;
- статистический анализ;
- статистическая оценка качества.

Первые два метода можно отнести к основным, которые непосредственно используются при управлении качеством, а два последних - как вспомогательные при решении задач двумя предыдущими.

Для эффективного использования технологических методов ведущее место занимает метрологическое обеспечение. При реализации технологических методов управления качеством часто используют графические методы, в том числе метод контрольных карт. Графики, построенные в виде контрольных карт, отличаются от обычных наличием специфических линий на них, которые указывают границы регулирования (контрольные границы). Контрольные карты используются при контроле качества продукции и регулировании технологических процессов. В зависимости от вида контроля различают контрольные карты по количественному (в том числе альтернативному) и качественному признакам. В первом случае используются численные значения показателей качества всей группы единиц продукции, во втором - всю группу единиц продукции делят на несколько подгрупп и решение о контролируемой партии принимают в зависимости от соотношений качества различных подгрупп. При использовании метода статистического анализа часто находят применение диаграммы Парето. Он наиболее часто используется при выявлении причин и факторов, позитивно или негативно влияющих на обеспечение и эффективность управления качеством, наглядно показывая при этом значимость каждой из причин или фактора в порядке уменьшения. В частности, с помощью этих диаграмм можно по всем видам брака для конкретной продукции объективно и полно оценить потери предприятия и установить важность тех или иных факторов в показателях качества продукции. Этот метод является также эффективным средством выработки управляющих воздействий в целях обеспечения уровня качества разрабатываемой и изготавливаемой продукции, профилактики и предупреждения брака на производстве. Диаграммы Парето дают возможность объективно показать фактическое состояние производства на отдельных участках и решить целый комплекс вопросов, связанных с качеством.

В том числе определить:

- число случаев брака по его видам;
- суммы потерь от брака;
- [затраты](http://center-yf.ru/data/Buhgalteru/Zatraty.php) времени и материальных средств на исключение брака;
- содержание поступающих рекламаций;
- число случаев отказа изделий в процессе их транспортирования;
- затраты, обусловленные удовлетворением рекламаций и т.д.

Кроме этого, они позволяют найти суммы по отдельным статьям производственной сметы, затраты на производство (сырье и материалы, вспомогательные материалы, затраты труда) и др. Следует отметить, что развитие в России рыночных отношений объективно требует более широкого использования [экономических методов](http://center-yf.ru/data/economy/Ekonomicheskie-metody.php) УК. Это является важнейшим условием выживания и процветания предприятий в рыночных отношениях.

Сущность экономического метода управления качеством

Экономические методы управления базируются на действии экономических механизмов мотивации и стимулирования активной производственной (реже - непроизводственной) деятельности. В отличие от организационно-административных эти методы управления ориентированы не столько на административное влияние (указы, распоряжения, указания и т.п.), сколько на экономическое стимулирование и вознаграждение за активную и эффективную деятельность. Значимость экономических методов управления резко возрастает в условиях развития рыночных отношений, ориентированных на получение прибыли и возможно более высокого дохода.

В группу экономических включают следующие методы управления качеством:

- финансирование деятельности в области управления качеством (кредитование разработок новаций в области управления качеством, новых и модернизируемых видов продукции; ссуды, определение стоимости, [калькуляция](http://center-yf.ru/data/economy/Kalkulyaciya.php), соизмерение затрат и результатов);
- хозяйственный расчет в подразделениях системы управления качеством;
- экономическое стимулирование производства, распределение и предоставление потребителям продукции и услуг, соответствующих их требованиям;
- [бизнес-планирование](http://center-yf.ru/data/Marketologu/Biznes-planirovanie.php) создания новых и модернизированных видов продукции и услуг, а также разработка соответствующих для них требованиям стандартизации и сертификации качества;
- [ценообразование](http://center-yf.ru/data/economy/Cenoobrazovanie.php) на продукцию и услуги с учетом их уровня качества;
- образование фондов экономического стимулирования качества, в том числе фондов поощрения и премирования за качество, создание и модернизация продукции, техники и технологии;
- применение [системы оплаты труда](http://center-yf.ru/data/Kadroviku/Sistema-oplaty-truda.php) и материального поощрения с учетом его качества на каждом [рабочем месте](http://center-yf.ru/data/Kadroviku/Rabochee-mesto.php) производственной системы и систему управления в целом;
- использование экономических мер воздействия на поставщиков в зависимости от качества поставляемой ими продукции и оказываемых услуг.

Один из примеров использования экономического метода - материальное стимулирование: в ответ на предварительно авансированное повышение [заработной платы](http://center-yf.ru/data/Kadroviku/Zarabotnaya-plata.php) можно ожидать более ответственного отношения работника к качеству своего труда, большего энтузиазма и как результат более высокого качества выпускаемой продукции. Такой подход можно сформулировать следующим образом: более высокая зарплата - более высокое качество продукции. Это противоречит ныне повсеместно используемому подходу высокая эффективность - высокая зарплата. Реализация этого подхода в широком масштабе может в итоге увеличить спрос и покупательские возможности населения (в связи с повышением зарплаты), что соответственно увеличивает объемы реализации продукции, валовой доход и массу прибыли предприятий (в том числе и того предприятия, где использован этот метод). Объемы продаж увеличиваются не только из-за повышения качества продукции, но и за счет уменьшения себестоимости (затем соответствующего снижения цены) и увеличения объемов производства. Все это станет вполне реальным следствием цивилизованных производственных отношений, взаимосвязанных с реализацией данного метода.

Сущность психологического метода управления качеством

Психологические методы управления качеством основаны на использовании группы факторов, влияющих на управление протекающими в трудовых коллективах социально-психологическими процессами для достижения целей в области качества.

Среди психологических методов следует отметить следующие:

- способы повышения самодисциплины, ответственности, инициативы и творческой активности каждого члена коллектива, а также коллективов подразделений по улучшению качества и совершенствованию управления им;
- формы морального стимулирования высокого качества результатов труда;
- приемы улучшения в коллективе психологического климата, включающие способы ликвидации конфликтов, рационального [стиля управления](http://center-yf.ru/data/Menedzheru/Stili-upravleniya.php) качеством, подбора и обеспечения психологической совместимости сотрудников;
- способы учета психологических особенностей членов трудовых коллективов при обеспечении качества;
- приемы формирования мотивов трудовой деятельности членов коллективов, направленных на достижение требуемого качества;
- способы сохранения и развития традиций предприятия по обеспечению необходимого качества;
- приемы вовлечения членов трудовых коллективов в управление качеством.

Современное состояние науки и техники позволяет осуществлять управление качеством разнообразными психологическими приемами, и исходных данных и исходного состояния предприятия.

**2. Теория принятия решений**

Человек наделён сознанием, существо свободное и обречено на выбор решений, стараясь сделать всё наилучшим образом. В наиболее общем смысле теория принятия оптимальных решений представляет собой совокупность математических и численных методов, ориентированных на нахождение наилучших вариантов из множества альтернатив и позволяющих избежать их полного перебора. Ввиду того, что размерность практических задач, как правило, достаточно велика, а расчеты в соответствии с алгоритмами оптимизации требуют значительных затрат времени, то методы принятия оптимальных решений главным образом ориентированы на реализацию их с помощью ЭВМ.

Практическая потребность общества в научных основах принятия решений возникла с развитием науки и техники только в XVIII веке Началом науки "Теория принятия решений" следует считать работу Жозефа Луи Лагранжа, смысл которой заключался в следующем: сколько земли должен брать на лопату землекоп, чтобы его сменная производительность была наибольшей. Оказалось, что утверждение "бери больше, кидай дальше" неверен. Бурный рост технического прогресса, особенно во время и после второй мировой войны, ставил все новые и новые задачи, для решения которых привлекались и разрабатывались новые научные методы. Можно выделить следующие научно-технические предпосылки становления "Теории принятия решений":

* *удорожание "цены ошибки".* Чем сложнее, дороже, масштабнее планируемое мероприятие, тем менее допустимы в нем "волевые" решения и тем важнее становятся научные методы, позволяющие заранее оценить последствия каждого решения, заранее исключить недопустимые варианты и рекомендовать наиболее удачные;
* *ускорение научно-технической революции техники и технологии*. Жизненный цикл технического изделия сократился настолько, что "опыт" не успевал накапливаться и требовалось применение более развитого математического аппарата в проектировании;
* *развитие ЭВМ.*Размерность и сложность реальных инженерных задач не позволяло использовать аналитические метода.

Как часто это бывает, эта наука, с одной стороны, стала определенной ветвью других более общих наук (теория систем, системный анализ, кибернетика и т.д.), а с другой, стала синтезом определенных фундаментальных более частных наук (исследование операций, оптимизация и т.д.), создав при этом и собственную методологию.

Инженерное дело теснейшим образом связано с совокупностями объектов, которые принято называть *сложными системами*, которые характеризуются многочисленными и разнообразными по типу связями между отдельно существующими элементами системы и наличием у системы функции назначения, которой нет у составляющих ее частей. На первый взгляд каждая сложная система имеет уникальную организацию. Однако более детальное изучение способно выделить общее в системе команд ЭВМ, в процессах проектирования лесной машины, самолета и космического корабля.

В научно-технической литературе существует ряд термином, имеющих отношение к исследованию сложных систем.

Наиболее общий термин "*теория систем*" относится ко всевозможным аспектам исследования систем. Ее основными частями являются

* *системный анализ*, который понимается как исследование проблемы принятия решения в сложной системе,
* *кибернетика*, которая рассматривается как наука об управлении и преобразовании информации.

Здесь следует заметить, что понятие *управления* не совпадает с *принятием решения*. Условная граница между кибернетикой и системным анализом состоит в том, что первая изучает отдельные и строго формализованные процессы, а системный анализ - совокупность процессов и процедур.

Очень близкое к термину "системный анализ" понятие - "*исследование операций*", которое традиционно обозначает математическую дисциплину, охватывающую исследование математических моделей для выбора величин, оптимизирующих заданную математическую конструкцию (критерий). Системный анализ может сводиться к решению ряда задач исследования операций, но обладает свойствами, не охватываемыми этой дисциплиной. Однако в зарубежной литературе термин "исследование операций" не является чисто математическим и приближается к термину "системный анализ". Широкая опора системного анализа на исследование операций приводит к таким его математизированным разделам, как

* постановка задач принятия решения;
* описание множества альтернатив;
* исследование многокритериальных задач;
* методы решения задач оптимизации;
* обработка экспертных оценок;
* работа с макромоделями системы.

*Системный анализ* - наука, занимающаяся проблемой принятия решения в условиях анализа большого количества информации различной природы.

Из определения следует, что целью применения системного анализа к конкретной проблеме является повышение степени обоснованности принимаемого решения, расширение множества вариантов, среди которых производится выбор, с одновременным указанием способов отбрасывания заведомо уступающим другим.

В системном анализе выделяют

* методологию;
* аппаратную реализацию;
* практические приложения.

*Методология*включает определения используемых понятий и принципы системного подхода.

Дадим основные определения системного анализа.

*Элемент* - некоторый объект (материальный, энергетический, информационный), который обладает рядом важных для нас свойств, но внутреннее строение (содержание) которого безотносительно к цели рассмотрения.

*Связь* - важный для целей рассмотрения обмен между элементами веществом, энергией, информацией.

*Система* - совокупность элементов, которая обладает следующими признаками:

* связями, которые позволяют посредством переходов по ним от элемента к элементу соединить два любых элемента совокупности;
* свойством, отличным от свойств отдельных элементов совокупности.

Практически любой объект с определенной точки зрения может быть рассмотрен как система. Вопрос состоит в том, насколько целесообразна такая точка зрения.

*Большая система* - система, которая включает значительное число однотипных элементов и однотипных связей. В качестве примера можно привести трубопровод. Элементами последнего будут участки между швами или опорами. Для расчетов на прочность по методу конечных элементов элементами системы считаются небольшие участки трубы, а связь имеет силовой (энергетический) характер - каждый элемент действует на соседние.

*Сложная система* - система, которая состоит из элементов разных типов и обладает разнородными связями между ними. В качестве примера можно привести ЭВМ, лесной трактор или судно.

*Автоматизированная система* - сложная система с определяющей ролью элементов двух типов:

* в виде технических средств;
* в виде действия человека.

Для сложной системы автоматизированный режим считается более предпочтительным, чем автоматический. Например, посадка самолета или захват дерева харвестерной головкой выполняется при участии человека, а автопилот или бортовой компьютер используется лишь на относительно простых операциях. Типична также ситуация, когда решение, выработанное техническими средствами, утверждается к исполнению человеком.

*Структура системы* - расчленение системы на группы элементов с указанием связей между ними, неизменное на все время рассмотрения и дающее представление о системе в целом. Указанное расчленение может иметь материальную, функциональную, алгоритмическую или другую основу. Пример материальной структуры - структурная схема сборного моста, которая состоит из отдельных, собираемых на месте секций и указывает только эти секции и порядок их соединения. Пример функциональной структуры - деление двигателя внутреннего сгорания на системы питания, смазки, охлаждения, передачи крутящего момента. Пример алгоритмической структуры - алгоритм программного средства, указывающего последовательность действий или инструкция, которая определяет действия при отыскании неисправности технического устройства.

Структура системы может быть охарактеризована по имеющимся в ней типам связей. Простейшими из них являются последовательное, параллельное соединение и обратная связь.

*Декомпозиция* - деление системы на части, удобное для каких-либо операций с этой системой. Примерами будут: разделение объекта на отдельно проектируемые части, зоны обслуживания; рассмотрение физического явления или математическое описание отдельно для данной части системы.

*Иерархия*- структура с наличием подчиненности, т.е. неравноправных связей между элементами, когда воздействие в одном из направлений оказывают гораздо большее влияние на элемент, чем в другом. Виды иерархических структур разнообразны, но важных для практики иерархических структур всего две - древовидная и ромбовидная .

Древовидная структура наиболее проста для анализа и реализации. Кроме того, в ней всегда удобно выделять иерархические уровни - группы элементов, находящиеся на одинаковом удалении от верхнего элемента. Пример древовидной структуры - задача проектирования технического объекта от его основных характеристик (верхний уровень) через проектирование основных частей, функциональных систем, групп агрегатов, механизмов до уровня отдельных деталей.

*Принципы системного подхода* - это положения общего характера, являющиеся обобщением опыта работы человека со сложными системами. Их часто считают ядром методологии. Известно около двух десятков таких принципов, ряд из которых целесообразно рассмотреть:

* принцип конечной цели: абсолютный приоритет конечной цели;
* принцип единства: совместное рассмотрение системы как целого и как совокупности элементов;
* принцип связности: рассмотрение любой части совместно с ее связями с окружением;
* принцип модульного построения: полезно выделение модулей в системе и рассмотрение ее как совокупности модулей;
* принцип иерархии: полезно введение иерархии элементов и(или) их ранжирование;
* принцип функциональности: совместное рассмотрение структуры и функции с приоритетом функции над структурой;
* принцип развития: учет изменяемости системы, ее способности к развитию, расширению, замене частей, накапливанию информации;
* принцип децентрализации: сочетание в принимаемых решениях и управлении централизации и децентрализации;
* принцип неопределенности: учет неопределенностей и случайностей в системе.

*Аппаратная реализация* включает стандартные приемы моделирования принятия решения в сложной системе и общие способы работы с этими моделями. Модель строится в виде связных множеств отдельных процедур. Системный анализ исследует как организацию таких множеств, так и вид отдельных процедур, которые максимально приспосабливают для принятия согласующихся и управленческих решений в сложной системе.

Модель принятия решения чаще всего изображается в виде схемы с ячейками, связями между ячейками и логическими переходами. Ячейки содержат конкретные действия - процедуры. Совместное изучение процедур и их организации вытекает из того, что без учета содержания и особенностей ячеек создание схем оказывается невозможным. Эти схемы определяют стратегию принятия решения в сложной системе. Именно с проработки связанного множества основных процедур принято начинать решение конкретной прикладной задачи.

Отдельные же процедуры (операции) принято классифицировать на *формализуемые* и *неформализуемые*. В отличие от большинства научных дисциплин, стремящихся к формализации, системный анализ допускает, что в определенных ситуациях неформализуемые решения, принимаемые человеком, являются более предпочтительными. Следовательно, системный анализ рассматривает в совокупности формализуемые и неформализуемые процедуры, и одной из его задач является определение их оптимального соотношения.

Формализуемые стороны отдельных операций лежат в области прикладной математики и использования ЭВМ. В ряде случаев математическими методами исследуется связное множество процедур и производится само моделирование принятие решения. Все это позволяет говорить о математической основе системного анализа. Такие области прикладной математики, как исследование операций и системное программирование, наиболее близки к системной постановке вопросов.

*Практическое приложение*системного анализа чрезвычайно обширно по содержанию. Важнейшими разделами являются научно-технические разработки и различные задачи экономики. Ссылки на системность исследований, анализа, подхода включает биологию, экологию, военное дело, психологию, социологию, медицину, управление государством и регионом, лесное и сельское хозяйство, обучение и многое другое.

**3. ПРИНЯТИЕ РЕШЕНИЙ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ**

 **Принятие решений при неопределенном риске.**

В условиях неопределенного риска принимающий решение не может оценить, какие состояния внешней среды будут оказывать существенное влияние на результаты, так как не знает вероятности их появления. Это связано с недостатком информации из-за невозможности ее получения, или трудности ее получения, или ее высокой стоимости, или, наконец, недостаточной квалификации лица, принимающего решения. Наивысшая неопределенность существует в политической, научной и военной среде. Например, Министерство обороны принимает решение о начале разработки нового вооружения. Неизвестно, какое оружие разрабатывает потенциальный противник, в каких условиях будет использоваться это оружие и будет ли оно вообще использоваться.

В хозяйственных организациях так же довольно часто принимаются решения в условиях неопределенного риска. Причины те же. Но устранить их проще, так как возможно собрать дополнительную информацию, повысить квалификацию руководителей. Если все же приходится принимать решение в условиях неопределенного риска, то первостепенную важность приобретает личность принимающего решение. На принятие решения оказывают влияние многие характеристики личности. Мы выделим важнейшие:

1. Человек, принимающий решение, - оптимист. Такой человек склонен рассматривать происходящие события оптимистично. Да, могут быть разные стечения обстоятельств, какие то из них могут привести к неблагоприятным результатам. Но он верит, что к нему судьба благоволит и ему будет сопутствовать удача. Поэтому он рискует, объясняя свои решения крылатой фразой «кто не рискует, тот не пьет шампанского».
2. Человек, принимающий решение, - пессимист. Такой человек не склонен к риску, он ищет вариант решения, который обеспечивает пусть не очень большой, но верный положительный результат. Он действует по правилу «лучше иметь синицу в руках, чем журавля в небе».
3. Человек, принимающий решение, стремится к минимизации разочарования. Такой человек настроен на минимизацию упущенной выгоды. К примеру, в магазине подготовили к продаже определенное количество автомобилей, однако, спрос превысил предложение, некоторым покупателям пришлось отказать. Магазин имеет потери в виде упущенной выгоды. Если бы было подготовлено к продаже больше автомобилей, то доход был бы выше.
4. Человек, принимающий решение, не склонен к глубокому анализу последствий. В результате упрощается процесс принятия решений. Поскольку отсутствует информация о преимуществах какого – либо варианта решения, то все варианты имеют одинаковые шансы на существование, поэтому присваиваются одинаковые вероятности всем имеющимся вариантам решения. Дальше можно использовать весьма плодотворные методы теории вероятностей для обоснования выбора решения, однако, надеяться на хороший результат нельзя, так как не предприняты усилия по анализу внешней среды, не определены вероятности наступления каждого ее состояния.

Правила принятия решений без использования численных значений вероятностей исходов (при неопределенном риске)

1. Максимаксное решение – поиск варианта, позволяющего получить максимальный доход.
2. Максиминное решение – поиск варианта, позволяющего получить пусть небольшой, но верный доход.
3. Минимаксное решение - поиск варианта, позволяющего получить минимальные потери.

Использование этих правил предполагает предварительный расчет платежной матрицы.

Платеж понимается как денежное вознаграждение или полезность, являющиеся следствием использования конкретной стратегии и возникающие при действии определенных обстоятельств.

*Если построить таблицу, в столбцах показать возможные стратегии, а в строках – возможные ситуации, обстоятельства, то в результате получим упорядоченную таблицу, или матрицу, которая получила название платежной.* В каждой ячейке отражается платеж, который будет получен, если при определенной стратегии возникает указанное в строке обстоятельство.

Платежная матрица используется в том случае, если:

1. Имеется ограниченное число вариантов действий;
2. Решение принимается в условиях неопределенности или риска;
3. Решение зависит от варианта действий (стратегии) и имеющихся обстоятельств.

Покажем расчет платежной матрицы и использование указанных выше правил на примере.

Пример. Цветочный магазин «Ирис» закупает в ООО «Флора» готовые букеты по цене 160 рублей и продает их по цене 200 рублей. Если букеты в течение трех дней не будут куплены, то магазин организует распродажу букетов по цене 100 рублей. Возможные варианты продаж в течение трех дней от 3 до 9 букетов (цифры условные, приняты для упрощения расчетов).

Определить, сколько букетов следует заказывать в расчете на три дня работы.

*Решение.*

Прежде всего, необходимо построить платежную матрицу.

В столбцах покажем возможные варианты закупок магазином букетов для продажи. Поскольку реализация может быть от 3 до 9 букетов, то и закупать следует не меньше 3 и не больше 9 букетов. В строках покажем варианты спроса.

*Платежная матрица может строится как матрица дохода или матрица потерь.* Матрица дохода определяет прибыль, которую может получить предприятие, матрица потерь – упущенный доход. Упущенный доход может быть следствием того, что затраты фирмы превысят выручку и она понесет реальные потери. Но может быть и такая ситуация, когда спрос превысит предложение, фирма могла бы реализовать больше продукции или услуг, но не подготовилась к этому, возникают упущенные возможности, определяемые как упущенный доход.

Построим вначале матрицу дохода. Каждый элемент этой матрицы будет характеризовать доход или убыток, который будет иметь фирма при реализации определенной стратегии закупок, указанной в столбце, и определенном спросе, указанном в строке (см. табл. 11).

Таблица 11.

Доход (прибыль) за три дня, руб.

|  |  |
| --- | --- |
| Варианты продаж |  Количество закупленных букетов |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 3 | 120 | *60* | *0* | *-60* | *-120* | *-180* | *-240* |
| 4 | 120 | 160 | 100 | 40 | -20 | -80 | -140 |
| 5 | 120 | 160 | 200 | 140 | 80 | 20 | -40 |
| 6 | 120 | 160 | 200 | 240 | 180 | 120 | 60 |
| 7 | 120 | 160 | 200 | 240 | 280 | 220 | 160 |
| 8 | 120 | 160 | 200 | 240 | 280 | 320 | 260 |
| 9 | *120* | 160 | 200 | 240 | 280 | 320 |  360 |

Для каждой ситуации следует определить денежные потоки.

Так, если магазин купит 3 букета и все три букета будут проданы, то доход магазина составит:

2003 – 1603 = 120(руб.)

При закупке магазином 4 букетов и продаже 3 букетов прибыль магазина составит:

2003 + 100 – 1604 = 60 (руб.)

Три букета будут проданы по 200 руб., еще магазин получит 100 руб. при распродаже. Затраты магазина будут при покупке четырех букетов по 160 руб. каждый.

Рассмотрим дальше доход (убыток), который можно получить по 3-му варианту продаж:

При 5-ти закупленных букетах

2003 + 1002 – 1605 = 0 (руб.)

При 6-ти закупленных букетах

 2003 + 1003 – 1606 = -60 (руб.)

При 7-ми закупленных букетах

 2003 + 1004 – 1607 = -120 (руб.)

При 8-ми закупленных букетах

 2003 + 1005 – 1608 = -180 (руб.)

При 9-ти закупленных букетах

 2003 + 1006 – 1609 = -240 (руб.)

Если придет 4 покупателя, а в магазине будет только 3 букета, то доход составит:

 2003 – 1603 = 120 (руб.)

При 4-х покупателях и наличии 4 букетов доход будет:

2004 – 1604 = 160 (руб.)

Продолжая далее расчеты по 4-му варианту продаж, получаем:

 2004 + 100 – 1605 = 100 (руб.)

 2004 + 1002 – 1606 = 40 (руб.)

 2004 + 1003 – 1607 =-20 (руб.)

 2004 + 1004 – 1608 =-80 (руб.)

 2004 + 1005 – 1609 =-140 (руб.)

Аналогично определяются доходы (убытки) по остальным вариантам продаж. Результаты расчетов занесены в платежную матрицу.

Теперь покажем второй способ расчета платежной матрицы.

При продаже одного букета доход магазина равен 40 руб.

Если же букет куплен магазином, но не продан во время, то убытки будут равны 160 – 100 = 60 руб.

При 3-х закупленных и проданных букетах доход составит 403 = 120 руб. По всем другим вариантам продаж доход не изменится, так как всего в магазине 3 букета и четвертому, пятому и следующим покупателям придется отказать.

Если магазином будет куплено 4 букета, а придет только три покупателя, то доход составит 340 – 160 = 60 руб. При четырех покупателях доход будет 440 = 160 руб. При спросе пять, шесть и более букетов доход не изменится, составит 160 руб., так как в магазине было только 4 букета.

Таким же способом можно рассчитать все элементы платежной матрицы.

Теперь используем правила принятия решений для ответа на вопрос, сколько магазину закупать букетов?

* 1. Правило максимакса.

В каждом столбце надо *найти максимальное число*. В платежной матрице эти числа показаны жирным шрифтом. Далее *из этих чисел выбрать максимальное. Столбец, который содержит это число и определяет рекомендуемый для магазина вариант закупок.* Наибольшее число из выделенных 360, следовательно, магазину рекомендуется закупить 9 букетов. Это оптимистическое решение. Действительно, при этом варианте закупок можно получить максимальный доход – 360 руб. И это прельщает оптимиста, он игнорирует возможные потери, а они, как видно по этому столбцу платежной матрицы, могут быть значительными, рассчитывает на максимально возможный доход.

5.2. Правило максимина.

*В каждом столбце платежной матрицы надо найти минимальное число.* У нас эти числа выделены курсивом. Далее *из этих чисел необходимо выбрать максимальное.* *Столбец, в котором находится максимальное число, определяет решение.* Максимальное число из выделенных курсивом чисел – 120, следовательно, магазину по этому правилу нахождения решения будет дана рекомендация закупить 3 букета. Это правило пессимиста, обеспечивающее очень осторожный подход к выбору решения. Да, это решение дает магазину существенно меньший доход, всего 120 руб., но зато гарантированный. При всех стеченьях обстоятельств магазин меньше 120 руб. дохода не получит.

5.3. Правило минимакса.

*Использование этого правила позволяет получить решение, обеспечивающее минимальные потери возможного дохода. Для применения этого правила необходимо построить матрицу потерь.* В табл.12 представлена матрица потерь для нашего примера.

Таблица 12.

Возможные потери, руб.

|  |  |
| --- | --- |
| Вариантыпродаж |  Число закупленных букетов |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 3 | 0 | 60 | 120 | 180 | 240 | 300 | 360 |
| 4 | 40 | 0 | 60 | 120 | 180 | 240 | 300 |
| 5 | 80 | 40 | 0 | 60 | 120 | 180 | 240 |
| 6 | 120 | 80 | 40 | 0 | 60 | 120 | 180 |
| 7 | 160 | 120 | 80 | 40 | 0 | 60 | 120 |
| 8 | 200 | 160 | 120 | 80 | 40 | 0 | 60 |
| 9 | 240 | 200 | *160* | 120 | 80 | 40 | 0 |

Рассмотрим столбец, в котором отражены возможные потери магазина при поставке трех букетов. Если спрос будет равен наличию букетов, то магазин никаких потерь не несет. При превышении спроса над наличием возникают упущенные возможности. Так, если появился четвертый покупатель, то упущенный доход составит 200 – 160 = 40 руб., при спросе 5 букетов упущенный доход увеличится до 402 = 80 руб. Каждый следующий покупатель увеличивает упущенный доход на 40 руб.

Теперь рассмотрим столбец, в котором отражены варианты потерь при четырех закупленных магазином букетах. Если будет продано только три букета, а один пойдет на распродажу, то потери магазина составят 160 – 100 = 60 руб. Если будет продано четыре букета, то потерь нет. При спросе более четырех букетов потери будут связаны с упущенными возможностями: можно было заказать больше букетов, но упустили возможность. При появлении пятого покупателя потери составят 402 = 80 руб. Каждый новый покупатель – это дополнительные потери в 40 руб.

Таким образом, *при спросе, меньшем наличия в магазине букетов, возникают реальные потери – убытки от возврата непроданных букетов. При спросе, большем наличия в магазине букетов, возникают потери как упущенные возможности, упущенный доход.*

Выбор решения по правилу минимакса осуществляется следующим образом:

*В каждом столбце выделяются числа, определяющие самые большие значения потерь.* В табл. 12 это числа 240, 200, 160, 180, 240, 300, 360. *Среди этих чисел выбирается наименьшее. Столбец, которому принадлежит это число, определяет оптимальный вариант работы.* Наименьшее число в нашем примере – 160, оно принадлежит столбцу пяти закупленных букетов. Максимально возможные потери по этому варианту минимальны.

Решение задачи по правилу минимакса – магазину следует закупать пять букетов.

Выбор метода решения по рассмотренным правилам зависит от цели, которую ставит лицо, принимающее решение. Таким образом, *сначала надо четко определить, какую цель вы ставите, принимая решение, затем в соответствие с поставленной целью выбрать метод решения.*

5.4. Критерий Гурвица – компромиссный способ принятия решений.

Рассмотренные выше максимаксный и максиминный способы принятия решений дают, по сути, полярные результаты. Первый очень рискованный, но зато позволяющий получить максимальный доход, второй очень осторожный, но с небольшим доходом.

*Способ Гурвица позволяет получить компромиссное решение между оптимистичным максимаксом и пессимистичным максимином.*

Платежная матрица составляется обычным способом. В ней в каждом столбце находятся наибольшие и наименьшие элементы. Эти элементы объединяются в столбцы низкого и высокого дохода. Далее лицо, принимающее решение, устанавливает веса для каждого из вариантов дохода и умножает их на элементы соответствующих столбцов. Просуммировав полученные результаты по каждому варианту решения, получают в некотором смысле средний доход по вариантам. Математического доказательства достоверности полученного результата здесь нет. *Качество решения зависит от интуиции принимающего решение при установлении весов для наихудших и наилучших результатов.* По наилучшему результату определяется рекомендуемое решение.

Вновь рассмотрим пример с закупкой букетов. Из каждого толбца платежной матрицы, представленной в табл. 11, выпишем элементы самого большого и самого низкого дохода. Пусть весомость большого дохода 0,7, а низкого 0,3. Все расчеты проведем в табл. 13.

Таблица 13.

Метод Гурвица

|  |  |  |  |
| --- | --- | --- | --- |
| Количествозакупаемыхбукетов | Доход, руб. | Вес | Ожидаемый доход, руб. |
| высокий | низкий | 0,7 | 0,3 |
| 3 | 120 | 120 | 84 | 36 | 120 |
| 4 | 160 | 60 | 112 | 18 | 120 |
| 5 | 200 | 0 | 140 | 0 | 140 |
| 6 | 240 | -60 | 168 | -18 | 150 |
| 7 | 280 | -120 | 196 | -36 | 160 |
| 8 | 320 | -180 | 224 | -54 | 170 |
| 9 | 360 | -240 | 252 | -72 | 180 |

Наибольший доход в 180 руб. за три дня предполагается получить при закупке магазином 9 букетов. Этот вариант рекомендуется к использованию.

Покажем расчеты в последней строке табл. 13:

 Из табл.11 «Доход за три дня» выбираем столбец с 9 закупаемыми букетами. В этом столбце самое большое число 360, а самое маленькое –240. Умножаем первое на 0,7 (360 0,7 = 252), а второе на 0,3 (-240 0,3 = -72). Суммируем результаты 252 –72 = 180. Эта цифра характеризует ожидаемый средний доход магазина при закупке 9 букетов.

Ожидаемый средний доход при закупке 8 букетов

320 0,7 – 180 0,3 = 224 – 54 = 170 руб.

Контрольные вопросы

1. Сущность принятия решения в условиях определенности
2. Понятие определенного риска
3. Понятие неопределенного риска
4. Сущность принятия решения в условиях определенного риска
5. Сущность принятия решения в условиях неопределенного риска

Литература

1. Литвак Б.Г. Разработка управленческого решения. – М.: Дело, 2002. – 392с
2. Ременников В.В. Разработка управленческого решения./ Уч. Пособие. – М. ЮНИТИ-ДАНА, 2001
3. Смирнов Э.А. Разработка управленческих решений: Учебник для вузов. – М.: ЮНИТИ – ДАНА, 2000. – 271с.
4. Эддоус М., Стэнсфилд Р. Методы принятия решений. – М.: Аудит, ЮНИТИ, 1997. – 590с.

**Тема 3 Информационные системы и информационные технологии в управлении качеством**

**Информационные системы в управлении качеством НОП.**

Известно, что материальной базой для создания процессно – ориентированных информационных систем на наукоемких предприятиях может стать только полнофункциональная система, охватывающая весь жизненный цикл НОП и содержащая в своем составе все необходимые программно – технические средства.

Корпоративные информационные системы (КИС) предприятий, ориентированные на выпуск наукоемкой продукции, должны включать в себя, как минимум, следующие компоненты:

PLM (Product Life – cycle Management) – технология управления жизненным циклом продукта

CALS (Continuous Acquisition and Life – cycle Support) – система непрерывной информационной поддержки жизненного цикла продукта (изделия)

Work Flow – технология управления движением проекта

Интранет – технология создания внутренней корпоративной сети

Интернет – глобальная компьютерная сеть

BPM (Business Process Modeler) – технология моделирования бизнес – процессов

CASE (Computer Aided Software Engineering) – системы автоматизированной разработки программного обеспечения

DOORS (Dynamic Object – Oricnted Requirements System) – динамическая объектно-ориентированная система управления требованиям

SADT (Structured Analysis and Desigh Technique) – метод структурного анализа и проектирования

COCOMO (Constructive Cost Model) – конструктивная стоимостная модель изделия

PDM (Product Data Management) – технология управления данными продукта (изделия)

CAE/CAD/CAM (Computer Aided Engineering/Designing/Manufacturing) – средства компьютерной поддержки разработки / проектирования / производства

ERP (Enterprise Resource Planning) – системы планирования и управления ресурсами предприятия

SCM (Supply Chain Management) – системы управления процессом поставки (снабжения)

СРС (Collaborative Product Commerce) – системы поддержки совместного бизнеса при производстве и реализации продукта (изделия).

- CAD, CAE, CAM, CAID – системы компьютерной поддержки соответственно проектирования, инженерных расчетов и моделирования, подготовки производства, промышленного дизайна и виртуальной реальности.

- PDM – система управления проектными данными и данными об изделии.

- EDM – системы управления данными инженерных расчетов.

- ERP – интегрированные системы управления предприятием.

- EDMS – системы электронного документооборота и управления заданиями.

- LSAR – система логического обеспечения.

- IETM – система разработки и поддержки электронной эксплутационной документации.

- IPPD – интегрированная разработка продукции и процессов.

- PM – система управления проектами.

 - Офисные приложения – текстовые процессоры, электронные таблицы, презентационная графика, органайзеры и пр.

- развитые системы телекоммуникаций, реализующие совместную работу географически разделенных коллективов и групп на принципах «виртуального офиса».

Корпоративные информационные системы должны обеспечивать поддержку конструктивных, технологических, производственных, логистических, эксплутационных данных и данных о качестве, представляющих собой полное электронное описание изделия.

Процедуры обмена электронными данными в корпорации должны обеспечивать:

* обмен всеми данными об изделиях;
* отсутствие потерь и искажений информации в передаваемых данных;
* независимость от конкретных программно – технических реализаций.

Для создания информационных систем, способных обеспечить проектирование, изготовление и послепродажную поддержку изделий «в цифре», компаниями в частности BAAN, SAP, EDS, PTC, Dassault Systemes, MatrixOne и др. предлагаются различные проектные решения на базе PLM – решений.

Создание единой электронной информационной среды и применение современных технологий компьютерного моделирования и быстрого прототипирования на ранних этапах жизненного цикла изделия позволяет:

1. – обеспечить углубленный и всесторонний анализ конструктивных параметров проектируемого изделия;
2. – уменьшить общее число изменений в конструкции изделий и выполнить значительную часть их на более ранних стадиях проектирования, когда цена изменений не столь велика, а сам проект наиболее гибок;
3. – выполнить моделирование процессов изготовления, сборки и эксплуатации изделия;
4. – промоделировав на всем жизненном цикле множество различных вариантов конструктивно – технологических, логистических и др. решений, найти оптимальное их сочетание;
5. – оценить стоимостные и временные показатели на отдельных этапах и на всем протяжении жизненного цикла изделия а, в конечном итоге, сократить время выхода изделия на рынок и минимизировать его стоимость.

Таким образом PLM – решения - это производственная стратегия, позволяющая создавать корпоративные информационные системы виртуального предприятия на базе информационных технологий в целях повышения качества и конкурентоспособности сложной наукоемкой многономенклатурной продукции.

Новая организационная форма выполнения крупномасштабных и наукоемких проектов, получившая название «виртуальное предприятие», представляет собой географически удаленные друг от друга компании, связанные общим бизнес - процессами, которые объединяются в организационные структуры на период реализации проекта.

Очевидно, что некая компания может одновременно участвовать во множество различных проектов и входить в различные виртуальные предприятия. Однако PLM – решения зачастую отождествляют с реализацией интегрированной информационной среды для конструкторско – технологической подготовки производства изделий. Связано это с тем, что PLM – решения таких компаний, как РТС, EDS, Dassault Systemes и др., выросшие на базе систем автоматизированного проектирования , помимо CAD - и PDM – систем, включают интерфейсы с одной или несколькими системами CAD (Pro/ENGINEER, Unigraphics, Catia, SolidWorks, Solid Edge и др.) и интерфейс с ERP – системой.

Создание КИС является исключительно сложным проектом, в состав участников его, как правило, входят крупные промышленные компании и производители программных средств, лидирующие на рынке информационных технологий.

При этом наиболее актуальной останется проблема планирования уровня качества, контроля и управления качеством и документирование всех процессов и информации о качестве продукции. Основная цель процесса управления качеством продукции состоит в уменьшении риска отклонений от требуемых (наперед заданных) значений, обнаружений любых отклонений и принятии адекватных мер для их устранения. Так ля решения этих задач в рамках дискретного производства компания Вааn предлагает iBaan TQM – информационную систему управления качеством. Охватывающую основные и вспомогательные бизнес – процессы, причем не только в процессе производства, но и при проведении НИР, ОКР и послепродажного обслуживания. Функции и особенности iBaan TQM включают управление поставщиками; управление несоответствиями; управление контролем.

Управление поставщиками.

Надежность и качество поставщика – основа успеха любой компании. Система iBaan TQM предлагает инструментарий для оценки эффективности работы поставщиков:

1. Оценка эффективности поставщика. Осуществляется путем организации и контроля:
* отчетов по проверке продукции;
* сертификатов поставщика и актов заводского тестирования;
* входного контроля материалов, комплектующих вне зависимости от места их выполнения;
1. Возможность оперативного контроля (отслеживаемость).
2. Паспорт качества.
3. Статистический выборочный входной контроль.
4. Список одобренных поставщиков. Оценки качества измеряют фактическую эффективность работы поставщика и служат основой для составления списка «одобренных» поставщиков.

Управление несоответствиями

Периодически даже компании, наилучшим образом управляемые, принимают или производят «бракованные» изделия или изделия, не удовлетворяющие техническим спецификациям. Поэтому компаниям нужны эффективные средства для документирования и управления изделиями. Которые не соответствуют требованиям. Эффективные средства управления несоответствиями позволяют компаниям оперативно управлять отбракованными изделиями и в тоже время формировать «предысторию качества» для лучшего понимания этого процесса и возможности его усовершенствования. Так система iBaan TQM включает следующие особенности управления несоответствиями:

1. Коды причин. При возникновении «брака» или «несоответствия техническим спецификациям» используются коды причин для ответа на вопрос «Что произошло не так, как надо было бы?». Коды причин определяются компаниями для каждого из процессов.
2. Управление маршрутами. После присвоения кода причины необходима процедура. Определяющая дальнейшие действия по исправлению брака, то есть надо ответить на вопрос «Что делать потом?».
3. Отчеты о несоответствии. Детальные отчеты о несоответствии могут обновляться в реальном масштабе времени для поддержания прозрачности критических процессов.
4. Диаграммы Парето (распределение брака по причинам). iBaan TQM позволяет быстро генерировать диаграммы Парето, чтобы четко идентифицировать наиболее критические проблемы по качеству и обеспечить анализ и поиск возможностей по усовершенствованию качества и снижению себестоимости.
5. Коррекция. В систему iBaan TQM включены профилактические и коррекционные процедуры для сокращения потерь и оптимизации эффективности работы поставщика и производителя.

Управление контролем.

Для большинства компаний контроль выполняется в нескольких местах, а также у поставщика и у заказчика. Система iBaan TQM обеспечивает такие возможности управления контролем, которые гарантируют выпуск только сертифицированных материалов и изделий за счет тестирования в те моменты, которые определены в процедурах по контролю качества. Система iBaan TQM помогает компаниям управлять цепочкой качества от поставок материала до послепродажного обслуживаия и контролировать ее.

Система контроля управляет тестированием, которое инициируется в любом месте и включает следующие процедуры:

* Контроль в процессе работы. Контроль в процессе работы позволяет производственным оператора/контролерам подтверждать качество работы до передачи полуфабрикатов для дальнейшей обработки.
* Контроль управления процессом.
* Контроль запасов. Контроль для подтверждения качества изделий, находящихся на хранении или на складе.
* Контроль готовых изделий. Контроль готовых изделий позволяет производственным операторам/контролерам осуществлять проверку изделий на удовлетворение требованиям заказчика до поставки изделий. После утверждения одобренных тестовых результатов автоматически могут выпускаться сертификаты соответствия для заказчиков.
* Эксплутационный контроль.
* Ведение серийных номеров. Серийные номера могут быть введены, сгенерированы и управляемы в системе iBaan TQM.
* Централизованность. Система iBaan TQM позволяет централизовывать процедуры и процессы обеспечения качества в целях увеличения эффективности процедур контроля и управления знаниями для идентификации и усовершенствования процессов обеспечения качества.
* Технические спецификации и тесты. Каждая техническая спецификация и испытания автоматически запускаются при каждом контроле.
* Атрибуты. Для каждого вида контроля существует возможность определения «атрибутов», идентифицирующих наиболее важную информацию, которую компания хочет зафиксировать во время проведения контроля.
* Отслеживаемость 100% - ная отслеживаемость поддерживается на протяжении всего жизненного цикла изделия.
* Рабочие листы. Рабочие листы могут создаваться для каждого подразделения или индивидуально для контролера.
* Автоматизация. Система iBaan TQM интегрируется с системой EPR. Контролерам автоматически передаются уведомления, требования контроля, критерии приемки, тестовые процедуры и шаблоны ввода результата.
* Управление статистическим процессом через составление диаграмм доступно в реальном масштабе времени для получения данных по качеству (измерения, графика и статистика), чтобы информировать операторов и выводить предупреждения о необходимости настройки оборудования.
* Более быстрое решение проблемы. Элементы, вышедшие за пределы технических спецификации, автоматически подсвечиваются «красным», как только контролер вводит результаты контроля.
* Быстрый доступ к информации. Все результаты контроля и информация, включая цифровые фотографии, электронные таблицы, отсканированные документы и т.д., могут быть сохранены. Это позволяет реализовать «безбумажную» технологию и обеспечивает мгновенный доступ к необходимой информации (предыстории процессов).
* Возможность составления отчетности (с системой Crystal Reports). Каждая компания имеет свои собственные уникальные требования к ведению отчетности, которые могут быть быстро реализованы и при необходимости модифицированы для удовлетворения изменяющихся потребностей бизнеса.

Совместное управление качеством сTQM.

 сTQM помогает модернизировать бизнес процессы и ввести глобальные информационные сети предприятия, позволяя принимать более обоснованные решения на основе точного и всестороннего сбора данных.

сTQM объединяет всех участников производственного процесса – конструкторов, поставщиков, операторов, контролеров, управленцев, заказчиков. сTQM помогает создавать практически «бесшовную» интеграцию процессов и их участников для достижения общей цели – создания высококачественных продуктов.

Ниже приводятся основные элементы сTQM:

* Интеграционная структура – устойчивая, удобная в работе интеграционная структура, которая соединяет сTQM с существенными прикладными программами предприятия (ERP, PDM,…). сTQM интегрирована с системой Baan.
* Web – приложения. Часть функциональных возможностей в системах ERP (особенно это касается системы управления качеством) могут быть представлены как приложения на базе браузера. Это дает возможность распределять соответствующую информацию в реальном масштабе времени и осуществлять доступ пользователей, находящихся в разных местах организации или даже за пределами предприятия (поставщики, субподрядчики и т.д.).
* Функциональные возможности управления качеством. Система функциональных возможностей управления поставщиком помогает управлять всем процессом сертификации поставщика, включая получения одобрения, оценку рейтинга поставщика и управление проверкой.
* Интеллектуальный центр ведения бизнеса (Портал). По мере быстрого роста объема данных в многочисленных прикладных программах предприятия важно в любой точке и в любой момент времени иметь единое представление информации, имеющейся в приложениях.

Информационные технологи в обеспечении качества НОП

Стандарт ISO 8402 – 94 «Качество. Словарь» определяет качество как совокупность свойств характеристик продукта (изделия или услуги) относящихся к его способности удовлетворять установленные или предполагаемые потребности потребителя.

Другими словами, качество – это агрегированное восприятие потребителем свойств и характеристик продукта (функциональности, надежности, безопасности, комфортности, экологичности и пр.) в их неразрывной взаимосвязи на всем протяжении цикла владения (цена продажи плюс затраты на эксплуатацию, ремонты, модернизацию и пр.) являются базовыми понятиями, определяющими конкурентоспособность продукта, его позиционирование на том или ином сегменте рынка.

При создании новых образцов НОП стоимость владения рассматривается как целевое ограничение, в которое должны укладываться изделия и системы при безусловном соответствии заданным тактико – техническим характеристикам и показателям качества.

Качество, цена и эксплуатационные издержки потребителя формируются на проектно – производственной стадии жизненного цикла НОП и определяются степенью совершенства научно – исследовательской, конструкторской базы разработчика НОП. Производственной, организационной и управленческой составляющих бизнес – среды производителя.

Понятие «гарантированное обеспечение качества» как особого вида деятельности в проектно – производственной сфере современных предприятий появилось относительно недавно, что связано с кардинальными изменениями требований рынка.

Сегодня поставщик должен доказывать и демонстрировать потребителю наличие определенной степени совершенства, зрелости и устойчивости своей проектно – производственной и организационно – управленческой среды. В результате новых требований рынка появилось понятие «система качества» как совокупность организационных структур, правил, процедур и ресурсов поставщика по гарантированному обеспечению качества.

В сегодняшних условиях наличие у поставщика сертифицированной по требованиям стандартов ISO 9000 системы качества является своеобразным «пропуском» для выхода продукции на мировой рынок. Однако, российские предприятия ВПК, имеющие сертификаты соответствия собственных систем качества требованиям ISO 9000, до сих пор не способны обеспечить гарантированный стабильный уровень качества выпускаемой продукции. Причины такого положения заключаются в следующем:

1. Стандарты ISO 9000:2000 являются отражением рыночной модели экономики, многолетнего опыта западной корпоративной культуры управления и организации бизнеса. Без глубокого реформирования организационных структур отечественных предприятий и организаций, реинжиниринга их бизнес – процессов, гармонизации нормативной базы с требованиями международных и корпоративных стандартов нельзя говорить о реальном создании на отечественных предприятиях систем качества, адекватных современным системам качества.

2. Неправильное понимание роли и места системы качества в общей организационной структуре предприятия. Система качества рассматривается как отдельная функциональная подсистема предприятия, наряду с подсистемами материально-технического снабжения, подготовки производства и пр., то есть в роли прямой наследницы комплексной системы управления качеством продукции (КСУКП) советского периода. На самом деле качество является ядром организационной системы управления предприятием.

3. Чрезмерное увлечение формальной стороной создания систем качества (написание «Руководств по качеству», проведение аудитов, получение сертификатов и пр.).

4. «Фетишизация» требований стандартов ISO 9000, неправильное мнение о том, что их безусловное и реальное исполнение приведет к автоматическому повышению качества деятельности предприятия и выпускаемой им продукции. Стандарты ISO 9000:2000 носят очень общий, не зависящий от специфики деятельности конкретного предприятия, характер и регламентируют лишь минимальный набор безусловно необходимых функций и процедур. По оценкам американских экспертов. Соблюдение требований ISO 9000 только на 17% соответствует облику идеального предприятия. Остальные 83% должны «добираться» за счет других методологий обеспечения качества и совершенствования деятельности предприятия, которые в отечественной практике почти не применяются.

Такими методологиями являются:

- постоянный реинжиниринг бизнес – процессов (Business Process Reengineering, BPR);

- параллельный инжиниринг (Concurrent Engineering, CE);

- интегрированная разработка изделий и процессов (Integrated Product and Process Development, IPPD);

- непрерывная информационная поддержка жизненного цикла изделий (Continuous Acquisition and Life Cycle Support, CALS);

- тотальное управление качеством (Total Quality Management, TQM);

- интегрированная модель зрелости процессов (Capability Maturity Model Integration, CMMI).

Чем выше уровень зрелости компании, тем более предсказуемыми и управляемыми становятся процессы и, как следствие, более предсказуемо и качественно будут реализованы проекты.

5. Сужение проблемы обеспечения качества до единой «технической» составляющей вместо, по крайней мере, двух:

- первая составляющая («технологическая среда») – соответствие параметров конкретной единицы продукции заданным тактико – техническим требованиям. Обеспечивается технологической средой (технологии, оборудование, персонал, методы выходного контроля и испытаний), то есть процессами, создающими добавленную стоимость;

- вторая составляющая («бизнес - среда») – гарантированное обеспечение повторяемости качества при серийном изготовлении продукции. Обеспечивается системой организации и управления бизнес – процессами на всех этапах жизненного цикла продукции.

Таким образом, проблема гарантированного обеспечения качества продукции не сводится к созданию (а тем более к сертификации) системы качества. Соответствующей требованиям ISO 9000.

Как известно, что качество продукции – это производная от качества деятельности предприятия, качества его бизнес – процессов, технологического базиса и информационных технологий.

Обобщенная схема взаимного позиционирования качества продукции российского и западного ВПК представлена на рисунке 1, где в качестве осей координат выбраны уровни развития технологического базиса, бизнес – процессов и информационных технологий.

* Уровни зрелости бизнес- процессов
* Уровни технологического базиса:

Т1 – универсальное технологическое оборудование с ручным управлением, доля оборудования с ЧПУ первых поколений (с возрастом более 15 лет) не превышает 20 %. Технологические процессы контролируются либо по качеству продукции на выходе, либо по косвенным признакам. Отсутствуют средства объективного контроля и регулирования прямых параметров процессов.

Т2 – более 50% станочного парка составляет оборудование с ЧПУ традиционных компоновок с возрастом менее 10 лет. Технологические процессы имеют средства объективного контроля и регулирования прямых параметров, с автоматическим протоколированием хода процессов.

Т3 – более 90% станочного парка составляет оборудование с новыми интеллектуальными устройствами ЧПУ, в том числе на базе новых конструктивных решений (линейные приводы, мехатронные модули, параллельная кинематика и пр.). Технологические процессы изготовления каждой детали предварительно моделируются на специализированных встроенных САЕ – системах с автоматической корректировкой параметров по результатам моделирования. В целом технологическое оборудование обеспечивает гарантированную 100%-ную годность с первой же детали.

* Уровни используемых информационных технологий:

И1 – частичная автоматизация плановоучетных функций (заработная плата, материально-техническое снабжение, конструкторско – технологические спецификации и пр.). фрагментарное использование изолированных CAD – систем при проектировании изделий и подготовке производства. Обмен электронными данными системами отсутствует, документооборот предприятия полностью бумажный.

И2 – два основных «острова» автоматизации – система проектирования и подготовки производства изделий (CAD/CAM/CAE/PDM) и система управления ресурсами предприятия (MRP/ERP), плюс целый ряд автономных систем для решения отдельных функциональных задач. Документооборот предприятия носит смешанный (бумажно – электронный характер).

И3 – единая корпоративная информационная система на базе PLM – решения, состоящая из полностью интегрированных функциональных подсистем, охватывающих все стадии жизненного цикла продукции. Документооборот предприятия полностью электронный.

Тем не менее, из трех равных по значимости направления существует главное, способное стать своего рода «локомотивом» повышения качества и конкурентоспособности продукции – это информационные технологии. Именно информационные технологии являются сегодня связывающим элементом, интегрирующим технологическую среду и бизнес- среду предприятия в единое целое (табл. 1), именно они лежат в основе процессно – ориентированных методологий обеспечения качества и совершенствования деятельности предприятия.

Таблица 1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Уровни развития предприятий | Первоначальный(Уровень большей части предприятия российского ВПК. Качество продукции низкое и нестабильное) | Повторяемый(Уровень пре-дприятии - ли-деров рос-сийского ВПК. Качество про-дукции среднее но неста-бильное) | Определенный(Уровень боль-шинства запад-ных компаний. Среднее, ста-бильное ка-чество продук-ции) | Управляемый(Уровень ведущих запад-ных компаний. Стабильно вы-сокое качество продукции) | Оптимизируемый(Уровень мировых лидеров. Продукция задает «стандарт качества» среди аналогов) |
| Объект | Модель изделия | Конструкторско – технологическаядокументация (информация на бумаге) | Цифровая (в электронном виде) |
| Процесс | Спецификация основных и вспомогательных бизнес - процессов | Отсутствует спецификация | Отдельные модули iBaan, PDM | Интеграция продуктов iBaan(ERP, CRM, SCM) на базе iBaan PLM и OpenWorld | iBaan + MES |
| Среда | Проектирование | Человеко - ориентированные | CAD | CAD/CAE | CAD/CAE/САМ | CAD/CAE/САМ/CAID |
| Постановка на производства (технологическое проект - ние) | CAD/CAE | CAD/CAE/САМ |
| Производство | Тип оборудования | Универсальное оборудование | Оборудование с ЧПУ 2-го поколения | Оборудование с ЧПУ 3-го поколения | Оборудование с ЧПУ 4-го поколения | Оборудование с ЧПУ 5-го поколения |
|  | Управление оборудованием | Ручное > 90% | Цифровое > 30% | Цифровое > 50% | Цифровое > 90% | Цифровое > 100% |
|  | Контроль за отклонениями | По вторичным показателям, ручной | Периодически, ручной или частично автомати-зированный | Периодический, цифровой | Цифровой  | Цифровой  |
|  | Оптимизация процесса | Ручные  | Ручная или частично автоматизирована | Цифровая, непрерывная | Цифровая  |
|  | Вспомогательные процессы | Ручные или частично автоматизированные | Автоматизи-рованные |
| Измерения, контроль, испытания | Процесс  | Периодический выборочный | Непрерывный сплошной |
|  | Результаты  |  |  |  |  |  |
| Послепродажная логистическая поддержка |  |  |  |  |  |

Контрольные вопросы к лекции 8

1. Информационные системы в управлении качеством
2. Совместное управление качеством сTQM
3. Современные методологии управления качеством
4. Что такое «гарантированное обеспечение качества»?
5. Характеристика стандартов ISO 9000: 2000
6. Что такое «уровни используемых информационных технологии»?
7. Дайте характеристику уровня развития технологического базиса, бизнес-процессов и информационных технологий?

**Тема 4. Экспертные системы в управлении качеством**

**1. Экспертные системы, их особенности**

**1.1. Определение экспертных систем, достоинство и назначение**

Экспертные системы - это яркое и быстро прогрессирующее направление в области искусственного интеллекта.

Искусственный интеллект – самое молодое научное направление. Появление его было подготовлено развитием мощности вычислительных машин.

Искусственный интеллект занимает исключительное положение. Это связано со следующим:

часть функций программирования в настоящее время оказалось возможным передать машине. При этом общение с машиной происходит на языке, близком к разговорному. Для этого в ЭВМ закладывают огромную базу знаний, способы решения, процедуры синтеза, программы, а также средства общения, позволяющие пользователю легко общаться с ЭВМ.

* в связи с внедрением ЭВМ во все сферы человеческой жизни становится возможным переход к безбумажной технологии обработки информации.
* если раньше производство ориентировалось на обязательное участие человека, то в настоящее время находят применение безлюдные технологии, основанные на роботизации и автоматизации системы управления.
* интеллектуальные системы в настоящее время начинают занимать ведущее положение в проектировании образцов изделий. Часть изделий невозможно спроектировать без их участия.

Системы, относящиеся к системам искусственного интеллекта в настоящее время:

* экспертные системы. Первые системы, которые нашли широкое применение. Их элементы используются в системах проектирования, диагностики, управления и играх. Основаны на вводе знаний высококвалифицированных специалистов (экспертов) в ЭВМ и разработке специальной системы по их использованию.
* системы естественно-языкового общения (подразумевается письменная речь). Данные системы позволяют производить обработку связанных текстов по какой-либо тематике на естественном языке.
* системы речевого общения.
* системы обработки визуальной информации. Находят применение в обработке аэрокосмических снимков, данных, поступающих с датчиков.
* системы машинного перевода. Подразумеваются естественные языки человеческого общения.

Экспертная система - это набор программ или программное обеспечение, которое выполняет функции эксперта при решении какой-либо задачи в области его компетенции. Экспертная система, как и эксперт-человек, в процессе своей работы оперирует со знаниями. Знания о предметной области, необходимые для работы экспертных систем, определённым образом формализованы и представлены в памяти ЭВМ в виде базы знаний, которая может изменяться и дополняться в процессе развития системы.

Экспертные системы выдают советы, проводят анализ, выполняют классификацию, дают консультации и ставят диагноз. Они ориентированы на решение задач, обычно требующих проведения экспертизы человеком-специалистом. В отличие от машинных программ, использующий процедурный анализ, экспертные системы решают задачи в узкой предметной области (конкретной области экспертизы) на основе дедуктивных рассуждений. Такие системы часто оказываются способными найти решение задач, которые неструктурированны и плохо определены. Они справляются с отсутствием структурированности путём привлечения эвристик, то есть правил, взятых «с потолка», что может быть полезным в тех системах, когда недостаток необходимых знаний или времени исключает возможность проведения полного анализа.

Главное достоинство экспертных систем - возможность накапливать знания, сохранять их длительное время, обновлять и тем самым обеспечивать относительную независимость конкретной организации от наличия в ней квалифицированных специалистов. Накопление знаний позволяет повышать квалификацию специалистов, работающих на предприятии, используя наилучшие, проверенные решения.

Практическое применение искусственного интеллекта на машиностроительных предприятиях и в экономике основано на экспертных системах, позволяющих повысить качество и сохранить время принятия решений, а также способствующих росту эффективности работы и повышению квалификации специалистов.

**1.2. Классификация экспертных систем**

Схема классификации

Класс «экспертные системы» сегодня объединяет несколько тысяч различных программных комплексов, которые можно классифицировать по различным критериям.

Классификация по решаемой задаче

Интерпретация данных. Это одна из традиционных задач для экспертных систем. Под интерпретацией понимается определение смысла данных, результаты которого должны быть согласованными и корректными. Обычно предусматривается многовариантный анализ данных.

Пример:

* обнаружение и идентификация различных типов океанских судов - SIAP;
* определение основных свойств личности по результатам психодиагностического тестирования в системах АВТАН-

ТЕСТ и МИКРОЛЮШЕР и других.

Диагностика. Под диагностикой понимается обнаружение неисправности в некоторой системе. Неисправность - это отклонение от нормы. Такая трактовка позволяет с единых теоретических позиций рассматривать и неисправность оборудования в технических системах, и заболевания живых организмов, и всевозможные природные аномалии. Важной спецификой является необходимость понимания функциональной структуры («анатомии») диагностирующей системы.

Пример:

* диагностика и терапия сужения коронарных сосудов - ANGY;
* диагностика ошибок в аппаратуре и математическом обеспечении ЭВМ - система СRIB и другие.

Мониторинг. Основная задача мониторинга - непрерывная интерпретация данных в I реальном масштабе времени и сигнализация о выходе тех или иных параметров за допустимые пределы. Главные проблемы – «пропуск» тревожной ситуации и инверсная задача «ложного» срабатывания. Сложность этих проблем в размытости симптомов тревожных ситуаций и необходимость учёта временного контекста.

Пример:

* контроль за работой электростанций СПРИНТ, помощь

диспетчерам атомного реактора - REACTOR;

* контроль аварийных датчиков на химическом заводе - FALCON и другие.

Проектирование. Проектирование состоит в подготовке спецификаций на создание «объектов» с заранее определёнными свойствами. Под спецификацией понимается весь набор необходимых документов - чертёж, пояснительная записка и так далее. Основные проблемы здесь - получение чёткого структурного описания знаний об объекте и проблема «следа». Для организации эффективного проектирования и, в ещё большей степени, перепроектирования необходимо формировать не только сами проектные решения, но и мотивы их принятия. Таким образом, в задачах проектирования тесно связываются два основных процесса, выполняемых в рамках соответствующей экспертной системы: процесс вывода и процесс объяснения.

Пример:

* проектирование конфигураций ЭВМ VАХ - 11/780 в системе ХСОN (или R1), проектирование БИС - САDHELР;
* синтез электрических цепей - SYN и другие.

Прогнозирование. Прогнозирующие системы логически выводят вероятные следствия из заданных ситуаций. В прогнозирующей системе обычно используется параметрическая динамическая модель, в которой значения параметров «подгоняются» под заданную ситуацию. Выводимые из этой модели следствия составляют основу для прогнозов с вероятностными оценками.

Пример:

* предсказание погоды - система WILLARD;
* оценки будущего урожая - РLANT;
* прогнозы в экономике - ЕСОN и другие.

Планирование. Под планированием понимается нахождение планов действий, относящихся к объектам, способным выполнять некоторые функции. В таких экспертных системах используются модели поведения реальных объектов с тем, чтобы логически вывести последствия планируемой деятельности.

Пример:

* планирование поведения робота - STRIPS;
* планирование промышленных заказов - ISIS;
* планирование эксперимента - МОLGЕN и другие.

Обучение. Системы обучения диагностируют ошибки при изучении какой-либо дисциплины с помощью ЭВМ и подсказывают правильные решения. Они аккумулируют знания о гипотетическом «ученике» и его характерных ошибках, затем в работе способны диагностировать слабости в знаниях обучаемых и находить соответствующие средства для их ликвидации. Кроме того, они планируют акт общения с учеником в зависимости от успехов ученика с целью передачи знаний.

Пример:

* обучение языку программирования Лисп в системе «Учитель Лиспа»;
* система РROUSТ - обучение языку Паскаль и другие.

В общем случае все системы, основанные на знаниях, можно подразделить на системы, решающие задачи анализа, и на системы, решающие задачи синтеза.Основное отличие задач анализа от задач синтеза заключается в следующем: если в задачах анализа множество решений может быть перечислено и включено в систему, то в задачах синтеза множество решений потенциально строится из решений компонентов или подпроблем. Задача анализа - это интерпретация данных, диагностика; к задачам синтеза относятся проектирование, планирование. Комбинированные задачи: обучение, мониторинг, прогнозирование.

Классификация по связи с реальным временем

Статические экспертные системы разрабатываются в предметных областях, в которых база знаний и интерпретируемые данные не меняются во времени. Они стабильны.

Пример.

Диагностика неисправностей в автомобиле.

Квазидинамические экспертные системыинтерпретируют ситуацию, которая меняется с некоторым фиксированным интервалом времени.

Пример. Микробиологические экспертные системы, в которых снимаются лабораторные измерения с технологического процесса один раз в 4-5 ч. (например, производство лизина) и анализируется динамика полученных показателей по отношению к предыдущему измерению.

Динамические экспертные системыработают в сопряжении с датчиками объектов в режиме реального времени с непрерывной интерпретацией поступаемых данных.

Пример. Управление гибкими производственными комплексами, мониторинг в реанимационных палатах и так далее.

Классификация по типу ЭВМ

На сегодняшний день существуют:

* экспертные системы для уникальных стратегически важных задач на суперЭВМ (Эльбрус, CRAY, CONVEX и другие.);
* экспертные системы на ЭВМ средней производительности (типа mainfrave);
* экспертные системы на символьных процессорах и рабочих станциях (SUN, АРОLLО);
* экспертные системы на мини- и супермини-ЭВМ (VАХ, micro-VАХ и другие);
* экспертные системы на персональных компьютерах (IВМ РС, МАС II и подобные).

Классификация по степени интеграции с другими программами

Автономные экспертные системы работают непосредственно в режиме консультаций с пользователем для специфических «экспертных» задач, для решения которых не требуется привлекать традиционные методы обработки данных (расчёты, моделирование и так далее.).

Гибридные экспертные системыпредставляют программный комплекс, агрегирующий стандартные пакеты прикладных программ (например, математическую статистику, линейное программирование или системы управления базами данных) и средства манипулирования знаниями. Это может быть интеллектуальная надстройка над ППП или интегрированная среда для решения сложной задачи с элементами экспертных знаний.

Несмотря на внешнюю привлекательность гибридного подхода, следует отметить, что разработка таких систем являет собой задачу, на порядок более сложную, чем разработка автономной экспертной системы. Стыковка не просто разных пакетов, а разных методологий (что происходит в гибридных системах) порождает целый комплекс теоретических и практических трудностей.

1.3. Отличие экспертных систем от традиционных программ

Один из способов определить экспертные системы - это сравнить их с обычными программами. Главное различие состоит в том, что экспертные системы манипулируют знаниями*,* тогда как обычные программы манипулируют данными.Фирма Теknowledge, которая занимается производством коммерческих экспертных систем, описывает эти различия, как показано в следующей таблице.

|  |  |
| --- | --- |
| Обработка данных | Инженерия знаний |
| Представление и использование данныхАлгоритмыПовторный прогонЭффективная обработка больших баз данных | Представление и использование знанийЭвристикиПроцесс логического выводаЭффективная обработка баз знаний |

Специалисты в области искусственного интеллекта имеют несколько более узкое (и более сложное) представление о том, что такое экспертная система. Под экспертной системой понимается программа для ЭВМ, обладающая следующими свойствами.

Компетентность. Экспертная система должна демонстрировать компетентность, то есть достигать в конкретной предметной области того же уровня профессионализма, что и эксперты-люди. Но просто уметь находить хорошие решения ещё недостаточно. Настоящие эксперты не только находят хорошие решения, но часто находят их очень быстро, тогда как новичкам для нахождения тех же решений, как правило, требуется намного больше времени. Следовательно, экспертная система должна быть умелой - она должна применять знания дляполучения решений эффективно и быстро,используя приёмы и ухищрения, какие применяют эксперты-люди, чтобы избежать громоздких или ненужных вычислений. Для того чтобы по-настоящему подражать поведению эксперта-человека, экспертная система должна обладать робастностъю. Этоподразумевает не только глубокое, но и достаточно широкое понимание предмета. А этого можно достичь, используя общие знания и методы нахождения решений проблем, чтобы уметь рассуждать исходя из фундаментальных принципов в случае некорректных данных или неполных наборов правил. Это один из наименее разработанных методов в современных экспертных системах, но именно им успешно пользуются эксперты-люди.

Символьные рассуждения. Эксперты, решая какие-то задачи (особенно

такого типа, для решения которых применяются экспертные системы), обходятся без решения систем уравнений или других трудоёмких математических вычислений. Вместо этого они с помощью символов представляют понятия предметной области и применяют различные стратегии и эвристики в процессе манипулирования этими понятиями. В экспертной системе знания тоже представляются в символьном виде, то есть наборами символов, соответствующих понятиям предметной области. В искусственном интеллекте символ *-* это строка знаков, соответствующая содержанию некоторого понятия реального мира.

Примеры символов:

Продукт

ответчик

0.8

Эти символы можно объединить, чтобы выразить отношения между ними. Когда эти отношения представлены в программе искусственного интеллекта, они называются символьными структурами.

Примеры символьных структур:

(ДЕФЕКТНЫЙ продукт)

(ВЫПУЩЕННЫЙ ответчиком продукт)

(РАВНО (ОТВЕТСТВЕННОСТЬ ответчик) 0.8)

Эти структуры можно интерпретировать следующим образом: «продукт является дефектным», «продукт был выпущен в продажу ответчиком» и «ответственность ответчика равна 0.8».

При решении задачи экспертная система вместо выполнения стандартных математических манипулирует этими символами. Нельзя сказать, что экспертная система вообще не производит математических расчётов, она их делает, но в основном она приспособлена для манипулирования символами. Вследствие подобного подхода представлениезнаний - выбор, форма и интерпретация используемых символов - становится очень важным. Кроме того, эксперты могут получить задачу, сформулированную неким произвольным образом, и преобразовать её к тому виду, который в наибольшей степени соответствует быстрому получению решения или гарантирует его максимальную эффективность. Эта способность переформулирования задачи- как раз то свойство, которое должно быть присуще экспертной системе для того, чтобы приблизить их мастерство к уровню экспертов-людей. К сожалению, большинство существующих в настоящее время экспертных систем не обладают этим свойством.

Глубина. Экспертная система должна иметь глубокие знания; это значит, что она способна работать эффективно в узкой предметной области, содержащей трудные, нетривиальные задачи. Поэтому правила в экспертной системе с необходимостью должны быть сложными либо в смысле сложности каждого правила, либо в смысле их обилия. Экспертные системы, как правило, работают с предметными областями реального мира, а не с тем, что специалисты в области искусственного интеллекта называют игрушечными предметными областями.В предметной области реального мира тот, кто решает задачу, применяет фактическую информацию к практической проблеме и находит решения, которые являются ценными с точки зрения некоторого критерия, определяющего соотношение стоимости и эффективности. В игрушечной предметной области либо задача подвергается чрезвычайному упрощению, либо производится нереалистическая адаптация некоторой сложной проблемы реального мира. Тот, кто решает такую проблему, обрабатывает искусственную информацию, которая в целях облегчения решения упрощена и порождает решения, имеющие чисто теоретический интерес.

В тех случаях, когда по отношению к сложной задаче или данным о ней сделаны существенные упрощения, полученное решение может оказаться неприменимым в масштабах, которые характерны для реальной проблемы. Рекомендации, методы представления знаний, организация знаний, необходимые для применения методов решения задач к этим знаниям, часто связаны с объёмом и сложностью пространства поиска,т.е. множества возможных промежуточных и окончательных решений задачи. Если проблема сверхупрощена или нереалистична, то размерность пространства поиска будет, скорее всего, резко уменьшена, и не возникнет проблем с быстродействием и эффективностью, столь характерных для реальных задач. Эта проблема размерности возникает столь естественно и неуловимо, что специалисты в искусственном интеллекте могут не оценить её истинные масштабы.

Самосознание. Экспертные системы имеют знания, позволяющие рассуждать об их собственных действиях, и структуру, упрощающую такие рассуждения. Например, если экспертная система основана на правилах, то ей легко просмотреть цепочки выводов, которые она порождает, чтобы прийти к решению задачи. Если заданы ещё и специальные правила, из которых ясно, что можно сделать с этими цепочками выводов, то можно использовать эти знания для проверки точности, устойчивости и правдоподобия решений задачи и даже построить доводы, оправдывающие или объясняющие процесс рассуждения. Это знание системы о том, как она рассуждает, называется метазнанием,что означает всего лишь знания о знаниях.

У большинства ныне существующих экспертных систем есть так называемый механизм объяснения.Это знания, необходимые для объяснения того, каким образом система пришла к данным решениям. Большинство этих объяснений включают демонстрацию цепочек выводов и доводов, объясняющих, на каком основании было применено каждое правило в цепочке. Возможность проверять собственные процессы рассуждения и объяснять свои действия - это одно из самых новаторских и важных свойств экспертных систем. Но почему это свойство так важно?

«Самосознание» так важно для экспертных систем потому, что: пользователи начинают больше доверять результатам, испытывать большую уверенность в системе;

ускоряется развитие системы, так как систему легче отлаживать;

предположения, положенные в основу работы системы, становятся явными, а не подразумеваемыми;

легче предсказывать и выявлять влияние изменений на работу системы.

Умение объяснить - это всего лишь один из аспектов самосознания. В будущем самосознание позволит экспертной системе делать даже больше. Они сами смогут создавать обоснования отдельных правил путём рассуждения, исходящего из основных принципов. Они будут приспосабливать свои объяснения к требованиям пользователя. Они смогут измерить собственную внутреннюю структуру путём коррекции правил, реорганизации базы знаний и реконфигурации системы.

Первый шаг в этом направлении - выделить метазнания и сделать их явными, точно так же как знания о предметной области выделены и сделаны явными. Ниже приведён пример метазнания - знания о том, как использовать предметные знания.

ЕСЛИ: к данной ситуации применимо несколько правил,

ТО: использовать сначала правила, предложенные экспертами, прежде чем прибегнуть к правилам, предложенным новичками.

Это метаправило говорит экспертной системе, каким образом она должна выбирать те правила, которые надо выполнить. Специалисты по искусственному интеллекту только начинают экспериментировать с формами представления метазнаний и их организацией в экспертных системах.

Экспертные системы делают ошибки. Существует очень важное отличие экспертных систем от традиционных программ. Тогда как традиционные программы разрабатываются таким образом, чтобы каждый раз порождать правильный результат, экспертные системы разработаны с тем, чтобы вести себя как эксперты, которые, как правило, дают правильные ответы, но иногда способны ошибаться.

На первый взгляд кажется, что в этом отношении программы имеют явное преимущество. Однако это преимущество кажущееся. Традиционные программы для решения сложных задач, напоминающих те, которые подходят для экспертных систем, тоже могут делать ошибки. Но их ошибки чрезвычайно трудно исправлять, поскольку стратегии, эвристики и принципы, лежащие в основе этих программ, явно не сформулированы в их тексте.Следовательно, эти ошибки нелегко определить и исправить. Подобно своим двойникам-людям экспертные системы могут делать ошибки. Но в отличие от обычных программ они имеют потенциальную способность учиться на своих ошибках. С помощью компетентных пользователей можно заставить экспертные системы совершенствовать своё умение решать задачи в ходе практической работы.

**1.4. Области применения экспертных систем**

Области применения систем, основанных на знаниях, могут быть сгруппированы в несколько основных классов: медицинская диагностика, контроль и управление, диагностика неисправностей в механических и электрических устройствах, обучение.

* Медицинская диагностика.

Диагностические системы используются для установления связи между нарушениями деятельности организма и их возможными причинами. Наиболее известна диагностическая система MYCIN, которая предназначена для диагностики и наблюдения за состоянием больного при менингите и бактериальных инфекциях. Её первая версия была разработана в Стенфордском университете в середине 70-х годов. В настоящее время эта система ставит диагноз на уровне врача-специалиста. Она имеет расширенную базу знаний, благодаря чему может применяться и в других областях медицины.

* Прогнозирование.

Прогнозирующие системы предсказывают возможные результаты или события на основе данных о текущем состоянии объекта. Программная система «Завоевание Уолл-стрита» может проанализировать конъюнктуру рынка и с помощью статистических методов алгоритмов разработать план капиталовложений на перспективу. Она не относится к числу систем, основанных на знаниях, поскольку использует процедуры и алгоритмы традиционного программирования. Хотя пока ещё отсутствуют экспертные системы, которые способны за счёт своей информации о конъюнктуре рынка помочь увеличить капитал, прогнозирующие системы уже сегодня могут предсказывать погоду, урожайность и поток пассажиров. Даже на персональном компьютере, установив простую систему, основанную на знаниях, можно получить местный прогноз погоды.

* Планирование.

Планирующие системы предназначены для достижения конкретных целей при решении задач с большим числом переменных. Дамасская фирма Informat впервые в торговой практике предоставляет в распоряжение покупателей 13 рабочих станций, установленных в холле своего офиса, на которых проводятся бесплатные 15-минутные консультации с целью помочь покупателям выбрать компьютер, в наибольшей степени отвечающий их потребностям и бюджету. Кроме того, компания Boeing применяет экспертные системы для проектирования космических станций, а также для выявления причин отказов самолётных двигателей и ремонта вертолётов. Экспертная система XCON, созданная фирмой DEC, служит для определения или изменения конфигурации компьютерных систем типа VAX и в соответствии с требованиями покупателя. Фирма DEC разрабатывает более мощную систему XSEL, включающую базу знаний системы XCON, с целью оказания помощи покупателям при выборе вычислительных систем с нужной конфигурацией. В отличие от XCON система XSEL является интерактивной.

* Интерпретация.

Интерпретирующие системы обладают способностью получать определенные заключения на основе результатов наблюдения. Система PROSPECTOR, одна из наиболее известных систем интерпретирующего типа, объединяет знания девяти экспертов. Используя сочетания девяти методов экспертизы, системе удалось обнаружить залежи руды стоимостью в миллион долларов, причём наличие этих залежей не предполагал ни один из девяти экспертов. Другая интерпретирующая система - HASP/SIAP. Она определяет местоположение и типы судов в тихом океане по данным акустических систем слежения.

* Контроль и управление.

Системы, основанные на знаниях, могут применяться в качестве интеллектуальных систем контроля и принимать решения, анализируя данные, поступающие от нескольких источников. Такие системы уже работают на атомных электростанциях, управляют воздушным движением и осуществляют медицинский контроль. Они могут быть также полезны при регулировании финансовой деятельности предприятия и оказывать помощь при выработке решений в критических ситуациях.

* Диагностика неисправностей в механических и электрических устройствах.

В этой сфере системы, основанные на знаниях, незаменимы как при ремонте механических и электрических машин (автомобилей, дизельных локомотивов и т.д.), так и при устранении неисправностей и ошибок в аппаратном и программном обеспечении компьютеров.

* Обучение.

Экспертные системы, выполняющие обучение, подвергают диагностике, «отладке» и исправлению (коррекции) поведение обучаемого. Примером является обучение студентов отысканию неисправностей в электрических цепях, обучение военных моряков обращению с двигателем на корабле и обучение студентов-медиков выбору антимикробной терапии. Обучающие системы создают модель того, что обучающийся знает и как он эти знания применяет к решению проблемы. Системы диагностируют и указывают обучающемуся его ошибки, анализируя модель и строя планы исправлений указанных ошибок. Они исправляют поведение обучающихся, выполняя эти планы с помощью непосредственных указаний обучающимся.

Большинство экспертных систем включают знания, по содержанию которых их можно отнести одновременно к нескольким типам. Например, обучающая система может также обладать знаниями, позволяющими выполнять диагностику и планирование. Она определяет способности обучаемого по основным направлениям курса, а затем с учетом полученных данных составляет учебный план. Управляющая система может применяться для целей контроля, диагностики, прогнозирования и планирования.

**2. Структура, этапы разработки экспертных систем**

**2.1.Основные компоненты экспертных систем**

Типичная экспертная система состоит из следующих основных компонентов: решателя (интерпретатора), рабочей памяти (РП), называемой также базой данных (БД), базы знаний (БЗ), компонентов приобретения знаний, объяснительного и диалогового компонентов (рисунок 1).

Интерфейс

пользователя

База знаний

Подсистема объяснений

Решатель

Интеллектуальный редактор базы знаний

Инженер + Эксперт по знаниям Пользователь

Рис. 1. Структура экспертной системы.

База данных предназначена для хранения исходных и промежуточных данных решаемой в текущий момент задачи. Этот термин совпадает по названию, но не по смыслу с термином, используемым в информационно-поисковых системах (ИПС) и системах управления базами данных (СУБД) для обозначения всех данных (и в первую очередь не текущих, а долгосрочных), хранимых в системе.

База знаний в экспертной системе предназначена для хранения долгосрочных данных, описывающих рассматриваемую область (а не текущих данных), и правил, описывающих целесообразные преобразования данных этой области.

Решатель, используя исходные данные из РП и знания из БЗ, формирует такую последовательность правил, которые, будучи применёнными к исходным данным, приводят к решению задачи.

Объяснительный компонент объясняет, как система получила решение задачи (или почему она не получила решения) и какие знания она при этом использовала, что облегчает эксперту тестирование системы и повышает доверие пользователя к полученному результату.

Диалоговый компонент ориентирован на организацию дружелюбного общения со всеми категориями пользователей как в ходе решения задач, так и приобретения знаний, объяснения результатов работы.

В разработке экспертной системы участвуют представители следующих специальностей:

эксперт в той проблемной области, задачи которой будет решать экспертная система;

инженер по знаниям - специалист по разработке экспертных систем;

программист - специалист по разработке инструментальных средств (ИС).

Необходимо отметить, что отсутствие среди участников разработки инженера по знаниям (то есть его замена программистом) либо приводит к неудаче процесс создания экспертной системы, либо значительно удлиняет его. Эксперт определяет знания (данные и правила), характеризующие проблемную область, обеспечивает полноту и правильность введения в экспертную систему знаний.

Инженер по знаниям помогает эксперту выявить и структурировать знания, необходимые для работы экспертной системы, осуществляет выбор того ИС, которое наиболее подходит для данной проблемной области, и определяет способ того представления знаний в этом ИС, выделяет и программирует (традиционными средствами) стандартные функции (типичные для данной проблемной области), которые будут использоваться в правилах, вводимых экспертом.

Программист разрабатывает ИС, содержащее в пределе все основные компоненты экспертной системы, осуществляет сопряжение ИС с той средой, в которой оно будет использовано.

Экспертная система работает в двух режимах: приобретения знаний и решения задач (называемом также режимом консультации или режимом использования экспертной системы).

В режиме приобретения знаний общение с экспертной системой осуществляется через посредничество инженера по знаниям. Эксперт описывает проблемную область в виде совокупности данных и правил. Данные определяют объекты, их характеристики и значения, существующие в области экспертизы. Правила определяют способы манипулирования данными, характерные для рассматриваемой проблемной области. Эксперт, используя компонент приобретения знаний, наполняет систему знаниями, которые позволяют экспертной системе в режиме решения самостоятельно (без эксперта) решать задачи из проблемной области.

Важную роль в режиме приобретения знаний играет объяснительный компонент. Именно благодаря ему эксперт на этапе тестирования локализует причины неудачной работы экспертной системы, что позволяет эксперту целенаправленно модифицировать старые или вводить новые знания. Обычно объяснительный компонент сообщает следующее: как правильно используют информацию пользователя; почему искались или не использовались данные или правила; какие были сделаны выводы и так далее. Все объяснения делаются, как правило, на ограниченном естественном языке или языке графики.

Режиму приобретения знаний при традиционном подходе к разработке программ соответствуют этапы алгоритмизации, программирования и отладки, выполняемые программистом. В отличие от традиционного подхода разработку программ осуществляет эксперт (с помощью экспертной системы), не владеющий программированием, а не программист.

В режиме консультации общение с экспертной системой осуществляет конечный пользователь, которого интересует результат и (или) способ получения решения. Пользователь в зависимости от назначения экспертной системы может не быть специалистом в данной проблемной области, в этом случае он обращается к экспертной системе за советом, не умея получить ответ сам, или быть специалистом, в этом случае он обращается к экспертной системе, чтобы либо ускорить процесс получения результата, либо возложить на экспертную систему рутинную работу. Термин «пользователь» означает, что им является и эксперт, и инженер по знаниям, и программист. Поэтому, когда хотят подчеркнуть, что речь идёт о том, для кого делалась экспертная система, используют термин «конечный пользователь».

В режиме консультации данные о задаче пользователя обрабатываются диалоговым компонентом, который выполняет следующие действия:

распределяет роли участников (пользователя и экспертной системы) и организует их взаимодействие в процессе кооперативного решения задачи;

 преобразует данные пользователя о задаче, представленные на привычном для пользователя языке, на внутренний язык системы;

преобразует сообщения системы, представленные на внутреннем языке, в сообщения на языке, привычном для пользователя (обычно это ограниченный естественный язык или язык графики).

После обработки данные поступают в РП. На основе входных данных в РП, общих данных о проблемной области и правил из БЗ решатель (интерпретатор) формирует решение задачи.

В отличие от традиционных программ экспертная система в режиме решения задачи не только исполняет предписанную последовательность, но и предварительно формирует её. Если ответ экспертной системы не понятен пользователю, то он может потребовать объяснения, как ответ получен.

2.2. Классификация инструментальных средств экспертных систем

В широком толковании в инструментарий включают и аппаратуру, ориентированную на разработку экспертных систем (аппаратурный инструментарий).

На проектирование и создание одной экспертной системы раньше требовалось 20-30 чел.-лет. В настоящее время имеется ряд средств, ускоряющих создание экспертных систем. Эти средства называются инструментальными (ИС), или инструментарием. Использование ИС сокращает время разработки экспертных систем в 3 - 5 раз.

Экспертные системы выполняются на ЭВМ следующих типов: общего назначения; ПЭВМ; интеллектуальные рабочие станции (то есть рабочие станции типа San, Арроlо и др., снабжённые эффективными ИС для создания экспертной системы); последовательные символьные ЭВМ типа ЛИСП - машин (Symbolik-3670, А1рhа, Ехр1огег, Хегох 1100 и дугие) и ПРОЛОГ - машин; параллельные символьные ЭВМ (Connection, Dado, Faun, Hyper Cube и другие).

Программные ИС определяются следующей совокупностью характеристик: назначение; стадия существования; тип ИС; тип используемых методов и знаний; универсальность; основные свойства; среда функционирования.

Назначение определяет, для работы в каких проблемных областях и для создания какой стадии экспертной системы предназначено ИС.

По степени отработанности ИС обычно выделяют три стадии существования: экспериментальная, исследовательская, коммерческая. Экспериментальные ИС создаются для решения узких специфических задач и редко проверяются на других задачах, обычно они работают медленно и неэффективно. Следующей стадией является исследовательская. Средства, достигшие этой стадии, обычно тщательно проверены, имеют документацию и поддерживаются разработчиком, однако они ещё могут действовать медленно и неэффективно. Исследовательские ИС используются при разработке прототипов экспертных систем. Высшей стадией существования ИС является коммерческая. Этой стадии достигают те ИС, которые всесторонне и тщательно проверены, хорошо документированы, сопровождаются разработчиком, являются быстрыми и обладают удобным интерфейсом с пользователем.

По типу ИС классифицируются следующим образом:

* символьные языки программирования, ориентированные на создание экспертных систем и систем искусственного интеллекта (например, LISP, INTRLISP, SMALLTALK);
* языки инженерии знаний, т.е. языки высокого уровня, ориентированные на построение экспертных систем (например, ОРS-5, LOOPS, КЕS, ПРОЛОГ);
* системы, автоматизирующие разработку (проектирование) экспертных систем, (например, КЕЕ, АRТ, ТЕIRЕSIAS, АGЕ, ТIММ), их часто называют окружение (еnvironment) для разработки систем ИИ, ориентированных на знания;
* оболочки экспертных систем (или пустые экспертные) – экспертные системы, не содержащие знаний ни о какой проблемной области (например, ЭКСПЕРТИЗА, ЕМYСIN,ЭКО, ЭКСПЕРТ).

В приведённой классификации ИС перечислены в порядке убывания трудозатрат, необходимых на создание с их помощью конкретной экспертной системы. Действительно, при использовании ИС первого типа в задачу разработчика входит программирование всех компонентов экспертной системы на языке довольно низкого уровня. Использование ИС второго типа позволяет значительно повысить уровень языка, что, как правило, приводит к некоторому снижению эффективности. Инструментальные средства третьего типа позволяют разработчику не программировать все или часть компонентов экспертной системы, а выбирать их из заранее составленного набора. При применении ИС четвертого типа разработчик ИС полностью освобождается от работ по созданию программ, так как берет готовую пустую экспертную систему.

При использовании ИС третьего и особенно четвертого типа могут возникнуть следующие проблемы: управляющие стратегии, вложенные в процедуры вывода ИС, могут не соответствовать методам решения, которые использует эксперт, взаимодействующий с данной экспертной системой, что может приводить к неэффективным, а возможно, и к неправильным решениям; язык представления знаний, принятый в ИС, может не подходить для данного приложения.

Развитие систем, автоматизирующих разработку экспертных систем, приводит к появлению ИС, которые можно назвать настраиваемыми оболочками. Эти ИС позволяют разработчику использовать оболочку не как нечто неизменное, а генерировать оболочку из множества механизмов, имеющихся в ИС. Типичными таймерами таких ИС являются КЕЕ, АRТ, ЭКСПЕРТИЗА, ГЛОБ.

Инструментальные средства можно классифицировать и по классам экспертных систем на: ИС для создания простых экспертных систем, ИС для создания сложных экспертных систем. В настоящее время, как правило, ИС первого типа разрабатываются на ПЭВМ, а второго - на символьных ЭВМ, ЭВМ общего назначения и интеллектуальных рабочих станциях.

По типу используемых методов и знаний ИС делятся, так же как и экспертные системы, на традиционные, использующие только методы и способы представления инженерии знаний, и гибридные, сочетающие подходы инженерии знаний с подходами, развитыми в традиционном программировании при представлении данных и использовании подпрограмм.

Универсальность задаётся совокупностью двух параметров: универсальностью представления знаний и универсальностью функционирования. Универсальность представления характеризует способ; (модель) представления знаний в ИС и принимает следующие значения: единое представление - ИС использует одну модель; интегральное представление - ИС допускает интегральное использование нескольких моделей; универсальное - ИС допускает интегральное использование всех основных моделей представления. К основным моделям представления относятся: правила (продукции); фреймы или семантические сети; логические модели (исчисление предикатов). Примерами ИС, в которых используется единое представление, является ПРОЛОГ, интегральное представление - СENTAUR, а универсальное - КЕЕ, АRТ.

Универсальность функционирования характеризует механизмы (парадигмы), определяющие, как в ИС задается поведение (функционирование) системы, и принимает следующие значения: единый механизм функционирования - ИС использует один механизм функционирования; интегральное функционирование - ИС допускает интегральное использование нескольких механизмов функционирования; универсальное функционирование - ИС допускает интегральное использование всех основных механизмов. К основным механизмам (парадигмам программирования) относятся: процедурное программирование; обратное программирование; программирование, ориентированное на данные; программирование, ориентированное на правила.

Процедурное программирование наиболее широко распространено среди существующих сегодня языков программирования (например, Си). Здесь явно выделяют два вида различных сущностей: процедуры, являющиеся тем, что задает поведение (функционирование) программы и выполняющие активную роль; данные, являющиеся тем, что обрабатывается способом, предписанным процедурами, и выполняющие пассивную роль. Способность составлять процедуры из команд (операторов) и вызывать их - ключ функционирования, использующего данную парадигму. Особенностью её являются боковые эффекты, возникающие в тех случаях, когда различные процедуры, использующие общие данные, независимо их изменяют.

Парадигма объектного программирования в отличие от процедурной не разделяет программу на процедуры и данные. Здесь программа организуется вокруг сущностей (объектов), которые включают локальные процедуры (методы) и локальные данные (переменные). Поведение (функционирование) в этой парадигме организуется путем пересылки сообщений между объектами. Объект, получив сообщение, осуществляет его локальную интерпретацию, основываясь на локальных процедурах и данных. Объектная парадигма удобна в тех приложениях, где взаимодействие сущностей сведено к унифицированным протоколам. Важным свойством языков, использующих данную парадигму, является сеть наследований, которая существенно упрощает определение новых объектов, почти подобных известным.

В обеих рассмотренных парадигмах активная роль в организации поведения отводится процедурам, а не данным. Причём процедура активизируется либо её вызовом, либо посылкой ей сообщения. Подобные способы задания поведения удобны для описания детерминированной последовательности действий либо одного процесса, либо нескольких, но строго взаимосвязанных процессов.

В программировании, ориентированном на данные, активную роль играют данные, а не процедуры. Здесь со структурами активных данных связывают некоторые процедуры (действия), которые активизируются тогда, когда осуществляется доступ к этим данным. Описанный механизм в некотором смысле обратный механизму посылки сообщений. Действительно, сообщение является явным способом указать объекту, какие действия следует выполнять (эти действия в качестве бокового эффекта могут изменить значения некоторых данных (племенных), а отнесение данных к активным является явным способом указания на контроль за доступом к ним, при этом в качестве бокового эффекта может быть послано сообщение процедуре. Программирование, ориентированное на данные, позволяет организовать поведение малозависимых процессов, что трудно реализовать в процедурной и объектной парадигмах. Малая зависимость процессов означает, что они могут рассматриваться и программироваться отдельно. Однако, при использований парадигмы, управляемой данными, эти независимо запрограммированные процессы могут взаимодействовать между собой без их изменения, то есть без перепрограммирования.

В программировании, ориентированном на правила, поведение определяется множеством правил вида условие - действие. Условие задаёт образ данных, при возникновении которого действие правила может быть выполнено. Правила в данной парадигме играют такую же роль, как и подпрограммы в процедурной парадигме. Однако, если в процедурной парадигме поведение задаётся детерминированной последовательностью процедур, не зависящей (для широкого класса обрабатываемых данных) от значений этих данных, то в парадигме, ориентированной на правила, поведение (последовательность действий) задаётся не заранее предписанной последовательностью правил, а формируется на основе тех данных и их значений, которые в текущий момент обрабатываются программой (системой). Формирование поведения осуществляется по следующей схеме. Условия правил сопоставляются с текущими данными, и те правила, условия которых удовлетворяются значениями текущих данных, становятся претендентами на выполнение. Затем по определённому критерию осуществляется выбор одного правила среди претендентов и выполнение его (то есть выполнение действия, указанного в правой части правила). Если система (устройство) допускает параллельную обработку, то все правила-претенденты могут выполняться одновременно. Таким образом, правила выполняются в порядке, предписываемом теми образцами данных, которые, как правило, малозависимы друг от друга. Итак, подход, ориентированный на правила, удобен для описания поведения, гибко и разнообразно реагирующего на большое многообразие состояний данных. Основные свойства определяют особенности ИС с точки зрения реализации компонентов экспертных систем. Среда функционирования определяет тип ЭВМ, на которой реализовано ИС, тип операционной системы, в среде которой ИС работает, и используемый язык программирования.

**2.3. Организация знаний в экспертных системах**

Для специалистов в области искусственного интеллекта термин знанияозначает информацию, которая необходима программе, чтобы она вела себя «интеллектуально». Эта информация принимает форму фактов или правил.

Факты и правила в экспертной системе не всегда либо истинны, либо ложны; иногда существует некоторая степень неуверенности в достоверности факта или точности правила. Если это сомнение выражено явно, то оно называется «коэффициентом уверенности».

Многие правила экспертной системы являются эвристиками, то есть эмпирическими правилами или упрощениями, которые эффективно ограничивают поиск решения. Экспертная система использует эвристики, потому что задачи, которые она решает, будь то поиск новых месторождений или согласование исков, как правило, трудны и не до конца понятны. Эти задачи не поддаются строгому математическому анализу или алгоритмическому решению. Алгоритмический метод гарантирует корректное или оптимальное решение задачи, тогда как эвристический метод даёт приемлемое решение в большинстве случаев.

На рисунке 2 показано различие между алгоритмическим и эвристическим методами. Здесь сравнивается алгоритм предотвращения захвата самолётов на коммерческих авиалиниях с эвристическим методом, предназначенным для той же цели.

Предотвратить захват самолётов на коммерческих авиалиниях

Предотвратить посадку терро-ристов на самолёт

Алгоритм

Пропустить всех пассажиров и багаж через детектор металла. Обыскать только тех пассажиров, на которых реагирует детектор, а также тех, чьи приметы совпадают с предполагаемым обликом терро-риста (возраст, одежда, поведение и т. д.).

Провести личный досмотр каждого до-пускаемого на посадку в самолёт и обыскать весь багаж. Сюда входят все пассажиры, члены экипажа и механики.

Эвристика

Рис. 2. Алгоритмические и эвристические модели данных.

Алгоритм обеспечивает полную гарантию предотвращения захвата самолёта, потому что в принципе полностью исключает возможность проникновения оружия на борт самолёта. К сожалению, он требует слишком много времени, слишком дорог и, что ещё важнее; слишком непопулярен, чтобы иметь какую-либо практическую ценность. Приведенный эвристический метод также может предотвратить большинство попыток захвата самолётов, но не гарантирует, что они вообще не возникнут. Использование эвристических правил делает поиск решения намного более лёгким и более практичным.

Знания в экспертной системе организованы таким образом, чтобы знания о предметной области отделить от других типов знаний системы, таких, как общие знания о том, как решать задачи, или знания о том, как взаимодействовать с пользователем, например как печатать текст на терминале пользователя или как изменить текст в соответствии с командами пользователя. Выделенные знания о предметной области называются базой знаний,тогда как общие знания о нахождении решений задач называются механизмом вывода.

Программа, которая работает со знаниями, организованными подобным образом, называется системой, основанной на знаниях.

Программы искусственного интеллекта

Системы, основанные на знаниях

Экспертные системы

Демонстрируют интеллектуальное поведение умелым применением эвристик

Применяют экспертные знания к сложным задачам реальной жизни

Делают знания предметной области явными и отделяют их от остальной касты системы

Рис. 3. Экспертные системы как системы, основанные на знаниях.

Как показано на рисунке 3 , в сущности все экспертные системы являются системами, основанными на знаниях, но не наоборот. Программу искусственного интеллекта для игры в «крестики и нолики» нельзя будет считать экспертной системой, даже если в ней знания о предметной области отделить от остальной программы.

База знаний экспертной системы содержит факты (данные) и правила (или другие представления знаний), использующие эти факты как основу для принятия решений. Механизм вывода содержит интерпретатор, определяющий, каким образом применять правила для вывода новых знаний, и диспетчер, устанавливающий порядок применения этих правил. Такая структура экспертной системы показана на рисунке 4.

Экспертная система

База знаний (знания предметной области)

|  |
| --- |
| Факты |
| Правила |

|  |
| --- |
| Интерпретатор |
| Диспетчер |

Механизм вывода (общие знания о решении задач)

Рис. 4. Состав экспертной системы.

Выделение знаний о предметной области облегчает инженеру по знаниям разработку процедур для манипулирования ими. Каким образом система использует свои знания, имеет первостепенное значение, поскольку экспертная система должна иметь и адекватные знания, и средства эффективно использовать знания, чтобы её можно было считать умелойв каком-либо виде деятельности. Следовательно, для того, чтобы быть умелой, экспертная система должна иметь базу знаний, содержащую высококачественные знания о предметной области, а её механизм вывода должен содержать знания о том, как эффективно использовать знания о предметной области.

Концепция механизма вывода экспертной системы часто вызывает некоторое недоумение среди начинающих разработчиков. Обычно ясно, как знания предметной области могут быть записаны в виде фактов и правил, но далеко не ясно, каким образом конструировать и использовать так называемый «механизм вывода». Это недоумение происходит от отсутствия простого и общего метода организации логического вывода. Его структура зависит и от специфики предметной области и от того, как знания структурированы и организованы в экспертной системе. Многие языки высокого уровня, предназначенные для построения экспертных систем, например ЕМYСIМ, имеют механизм вывода, в некотором смысле встроенный в язык как его часть.

Другим примером может служить язык программирования Пролог со встроенным в него механизмом логического вывода, который может быть непосредственно использован при создании простых экспертных систем.

Языки более низкого уровня, например LISP, требуют, чтобы создатель экспертной системы спроектировал и реализовал механизм вывода.

Оба подхода имеют свои достоинства и недостатки. Язык высокого уровня со встроенным механизмом вывода облегчает работу создателя экспертной системы. В то же время у него, понятно, меньше возможностей определять способы организации знаний и доступа к ним, и ему следует очень внимательно рассмотреть вопрос о том, годится или нет на самом деле предлагаемая схема управления процессом поиска решения для данной предметной области. Использование языка более низкого уровня без механизма вывода требует больших усилий на разработку, но позволяет разработать нужные программные блоки, которые разработчик может встроить в схему управления процессом решения, который будет адекватен данной предметной области.

Что касается механизма вывода, то здесь дело не ограничивается выбором «всё или ничего». Так, некоторые инструменты построения экспертных систем имеют набор встроенных механизмов вывода, но позволяют разработчику модифицировать или переопределять их для большего соответствия с предметной областью.

 Существует много стандартных способов представления знаний, и при построении экспертных систем « может быть использован любой из них, сам по себе или в сочетании с другими. Каждый способ позволяет получить программу с некоторыми преимуществами - делает её более эффективной, облегчает её понимание и модификацию. В современных экспертных системах чаще всего используются три самых важных метода представления знаний: правила (самый популярный), семантическиесети и фреймы.

 Представление знаний, основанное на правилах, построено на использовании выражений вида ЕСЛИ (условие) *-* ТО (действие).Например:

(1) Если пациент был по профессии изолировщиком до 1988 г., то пациент непосредственно работал с асбестом. (2) Если пациент непосредственно работал с асбестом и пациент находился при этом в закрытом помещении, то пациент получил большую дозу асбестовой пыли. Когда текущая ситуация (факты) в задаче удовлетворяет или согласуется с частью правила ЕСЛИ, то выполняется действие, определяемое частью ТО. Это действие может оказаться воздействием на окружающий мир (например, вызовет распечатку текста на терминале пользователя), или же повлиять на управление программой (например, вызвать проверку и запуск некоторого набора правил), или может сводиться к указанию системе о получении определенного заключения (например, необходимо добавить новый факт или гипотезу в базу данных).

Сопоставление частей ЕСЛИ правил с фактами может породить так называемую цепочку выводов.Цепочка выводов, образованная последовательным применением правил 1 и 2, изображена на рисунке 5. Эта цепочка показывает, как система использует правила для вывода о том, насколько серьёзную дозу канцерогенного вещества пациент получил при работе с асбестом.

Рис. 5. Цепочка вывода для получения заключения о накопленной дозе асбестовой пыли.

Пациент был изолировщиком до 1988 г.

Пациент непосредственно работал с асбестом

Пациент контактировал с асбестом в закрытых помещениях

Пациент получил серьёзную дозу асбестовой пыли

Правила обеспечивают естественный способ описания процессов, управляемых сложной и быстро изменяющейся внешней средой. Через правила можно определять, как программа должна реагировать на изменение данных; при этом не нужно заранее знать блок-схему управления обработкой данных. В программе традиционного типа схема передачи управления и использования данных предопределена в самой программе. Обработка здесь осуществляется последовательными шагами, а ветвление имеет место только в заранее выбранных точках. Этот способ управления хорошо работает в случае задач, допускающих алгоритмическое решение, если к тому же при этом данные меняются достаточно медленно, например, при решении систем линейных уравнений. Для задач, ход решения которых управляется самими данными, где ветвление скорее норма, чем исключение, этот способ малоэффективен. В задачах такого рода правила дают возможность на каждом шаге оценить ситуацию и предпринять соответствующие действия. Использование правил упрощает объяснение того, что и как сделала программа, т. е. каким способом она пришла к конкретному заключению.

Представление знаний, основанное на фреймах, использует сеть узлов, связанных отношениями и организованных иерархически. Каждый узел представляет собой концепцию, которая может быть описана атрибутами и значениями, связанными с этим узлом. Узлы, которые занимают более низкое положение в иерархии, автоматически наследуют свойства узлов, занимающих более высокое положение. Эти методы обеспечивают естественный и эффективный путь классификации и построения таксономии, например залежей руд или различных заболеваний.

**2.4. Технология разработки экспертных систем**

Этапы разработки

Разработка программных комплексов экспертных систем как за рубежом, так и в нашей стране находится на уровне скорее искусства, чем науки. Это связано с тем, что долгое время системы искусственного интеллекта внедрялись в основном во время фазы проектирования, а чаще всего разрабатывалось несколько прототипных версий программ, прежде чем был получен конечный продукт. Такой подход действует хорошо в исследовательских условиях, однако в коммерческих условиях он является слишком дорогим, чтобы оправдать коммерчески жизненный продукт.

Процесс разработки промышленной экспертной системы, опираясь на традиционные технологии, можно разделить на шесть более или менее независимых этапов, практически не зависимых от предметной области.

Последовательность этапов дана для общего представления о создании идеального проекта. Конечно, последовательность эта не вполне фиксированная. В действительности каждый последующий этап разработки экспертной системы приносит новые идеи, которые могут повлиять на предыдущие решения и даже привести к их переработке. Именно поэтому многие специалисты по информатике весьма критично относятся к методологии экспертных систем. Они считают, что расходы на разработку таких систем очень большие, время разработки слишком длительное, а полученные в результате программы ложатся тяжёлым бременем на вычислительные ресурсы.

В целом за разработку экспертных систем целесообразно браться организации, где накоплен опыт по автоматизации рутинных процедур обработки информации, например:

* информационный поиск;
* сложные расчёты;
* графика;
* обработка текстов.

Решение таких задач, во-первых, подготавливает высококвалифицированных специалистов по информатике, необходимых для создания интеллектуальных систем, во-вторых, позволяет отделить от экспертных систем неэ

Этап 1: выбор подходящей проблемы

Этот этап включает деятельность, предшествующую решению начать разрабатывать конкретную экспертную систему. Он включает:

* определение проблемной области и задачи;
* нахождение эксперта, желающего сотрудничать при решении проблемы, и назначение коллектива разработчиков;
* определение предварительного подхода к решению проблемы;
* анализ расходов и прибыли от разработки;
* подготовку подробного плана разработки.

Правильный выбор проблемы представляет, наверное, самую критическую часть разработки в целом. Если выбрать неподходящую проблему, можно очень долгое время искать решение спроектированных задач. Неподходящая проблема может также привести к созданию экспертной системы, которая стоит намного больше, чем экономит. Дело будет обстоять ещё хуже, если разработать систему, которая работает, но не приемлема для пользователей. Даже если разработка выполняется самой организацией для собственных целей, эта фаза является подходящим моментом для получения рекомендаций извне, чтобы гарантировать удачно выбранный и осуществимый с технической точки зрения первоначальный проект.

При выборе области применения следует учитывать, что если знание, необходимое для решения задач, постоянное, чётко формулируемое и связано с вычислительной обработкой, то обычные алгоритмические программы, по всей вероятности, будут самым целесообразным способом решения проблем в этой области.

Экспертная система ни в коем случае не устранит потребность в реляционных базах данных, статистическом программном обеспечении, электронных таблицах и системах текстовой обработки. Но если результативность задачи зависит от знания, которое является субъективным, изменяющимся, символьным или вытекающим частично из соображений здравого смысла, тогда область может обоснованно выступать претендентом на экспертную систему.

Рассмотрим некоторые факты, свидетельствующие о необходимости разработки и внедрения экспертных систем:

* нехватка специалистов, расходующих значительное время для оказания помощи другим;
* потребность в многочисленном коллективе специалистов, поскольку;
* сниженная производительность, поскольку задача требует полного анализа сложного набора условий, а обычный специалист не в состоянии просмотреть (за отведённое время) все эти условия;
* большое расхождение между решениями самых хороших и самых плохих исполнителей;
* наличие конкурентов, имеющих преимущество в том, что они лучше справляются с поставленной задачей.

Подходящие задачи имеют следующие характеристики:

* являются узкоспециализированными;
* не зависят в значительной степени от общечеловеческих знаний или соображений здравого смысла;
* не являются для эксперта слишком лёгкими, ни слишком сложными (время, необходимое эксперту для решения проблемы, может составлять от трех часов до трех недель);
* условия исполнения задачи определяются самим пользователем системы;
* имеет результаты, которые можно оценить.

Обычно экспертные системы разрабатываются путём получения специфических знаний от эксперта и ввода их в систему. Некоторые системы могут содержать стратегии одного индивида. Следовательно, найти подходящего эксперта - это ключевой шаг в создании экспертных систем.

В процессе разработки и последующего расширения системы инженер по знаниям и эксперт обычно работают вместе. Инженер по знаниям помогает эксперту структурировать знания, определять и формализовать понятия и правила, необходимые для решения проблемы.

Во время первоначальных бесед они решают, будет ли их сотрудничество успешным. Это немаловажно, поскольку обе стороны будут работать вместе по меньшей мере в течение одного года. Кроме них в коллектив разработчиков целесообразно включить потенциальных пользователей и профессиональных программистов.

Предварительный подход к программной реализации задачи определяется исходя из характеристик задачи и ресурсов, выделенных на ее решение. Инженер по знаниям выдвигает обычно несколько вариантов, связанных с использованием имеющихся на рынке программных средств. Окончательный выбор возможен лишь на этапе разработки прототипа.

После того как задача определена, необходимо подсчитать расходы и прибыли от разработки экспертной системы. В расходы включаются затраты на оплату труда коллектива разработчиков. В дополнительные расходы включают стоимость приобретаемого программного инструментария, с помощью которого разрабатывается экспертная система.

Прибыль возможна за счёт снижения цены продукции, повышения производительности труда, расширения номенклатуры продукции или услуг или даже разработки новых видов продукции или услуг в этой области. Соответствующие расходы и прибыли от системы определяются относительно времени, в течение которого возвращаются средства, вложенные в разработку. На современном этапе большая часть фирм, развивающих крупные экспертные системы, предпочли разрабатывать дорогостоящие проекты, приносящие значительные прибыли.

Наметились тенденции разработки менее дорогостоящих систем, хотя и с более длительным сроком возвращаемости вложенных в них средств, так как программные средства разработки экспертных систем непрерывно совершенствуются.

После того как инженер по знаниям убедился, что:

* данная задача может быть решена с помощью экспертной системы;
* экспертную систему можно создать предлагаемыми на рынке средствами;
* имеется подходящий эксперт;
* предложенные критерии производительности являются разумными;
* затраты и срок их возвращаемости приемлемы для заказчика,

он составляет план разработки. План определяет шаги процесса разработки необходимые затраты, а также ожидаемые результаты.

Этап 2: разработка прототипной системы

Понятие прототипной системы

Прототипная системаявляется усечённой версией экспертной системы, спроектированной для проверки правильности кодирования фактов, связей и стратегий рассуждения эксперта. Она также даёт возможность инженеру по знаниям привлечь эксперта к активному участию в разработке экспертной системы и, следовательно, к принятию им обязательства приложить все усилия для создания системы в полном объёме.

Объём прототипа - несколько десятков правил, фреймов или примеров. Выделяют шесть стадий разработки прототипа. Рассмотрим краткую характеристику каждой из стадий.

Сроки приведены условно, так как зависят от квалификации специалистов и особенностей задачи.

Идентификация проблемы

Уточняется задача, планируется ход разработки прототипа экспертной системы, определяются:

* необходимые ресурсы (время, люди, ЭВМ и так далее.);
* источники знаний (книги, дополнительные эксперты, методики);
* имеющиеся аналогичные экспертные системы;
* цели (распространение опыта, автоматизация рутинных действий и другие);
* классы решаемых задач и так далее.

Идентификация проблемы - знакомство и обучение коллектива разработчиков, а также создание неформальной формулировки проблемы.

Средняя продолжительность 1 - 2 недели.

Извлечение знаний

Происходит перенос компетентности экспертов на инженеров по знаниям с использованием различных методов:

* анализ текстов;
* диалоги;
* экспертные игры;
* лекции;
* дискуссии;
* интервью;
* наблюдение и другие.

Извлечение знаний - получение инженером по знаниям наиболее полного представления предметной области и способах принятия решения в ней.

Средняя продолжительность 1 - 3 месяца.

Структурирование или концептуализация знаний

Выявляется структура полученных знаний о предметной области, то есть определяются:

* терминология;
* список основных понятий и их атрибутов;
* отношения между понятиями;
* структура входной и выходной информации;
* стратегия принятия решений;
* ограничения стратегий и так далее.

 Концептуализация знаний – разработка неформального описания знаний о предметной области в виде графа, таблицы, диаграммы или текста, которое отражает основные концепции и взаимосвязи между понятиями предметной области.

Средняя продолжительность этапа 2 – 4 недели.

Формализация

Строится формализованное представление концепций предметной области на основе выбранного языка представления знаний (ЯПЗ). Традиционно на этом этапе используются:

* логические методы (исчисления предикатов порядка и другие); продукционные модели (с прямым и обратным выводом); семантические сети;
* фреймы;
* объектно-ориентированные языки, основанные на иерархии классов, объектов и другие.

Формализация знания - разработка базы знаний на языке, который, с одной стороны, соответствует структуре поля знаний, а с другой - позволяет реализовать прототип системы на следующей стадии программной реализации.

Всё чаще на этой стадии используется симбиоз языков представления знаний, например, в системе ОМЕГА фреймы + семантические сети + полный набор возможностей языка исчисления предикатов.

Средняя продолжительность 1 - 2 месяца.

Реализация

Создаётся прототип экспертной системы, включающий базу знаний и остальные блоки, при помощи одного из следующих способов:

* программирование на традиционных языках типа Паскаль, Си и других; программирование на специализированных языках, применяемых в задачах искусственного интеллекта: LISP, FRL, SmallTalk и другие;
* использование инструментальных средств разработки экспертных систем типа СПЭИС, ПИЭС;
* использование «пустых» экспертных систем или «оболочек» типа ЭКСПЕРТ, ФИАКР и др.

Реализация - разработка программного комплекса, демонстрирующего жизнеспособность подхода в целом. Чаще всего первый прототип отбрасывается на этапе реализации действующей экспертной системы.

Средняя продолжительность 1 - 2 месяца.

Тестирование

Оценивается и проверяется работа программ прототипа с целью приведения в соответствие с реальными запросами пользователей. Прототип проверяется на:

* удобство и адекватность интерфейсов ввода-вывода (характер вопросов в диалоге, связность выводимого текста результата и другое);
* эффективность стратегии управления (порядок перебора, использование нечёткого вывода и другое);
* качество проверочных примеров;
* корректность базы знаний (полнота и непротиворечивость правил).

Тестирование - выявление ошибок в подходе и реализации прототипа и выработка рекомендаций по доводке системы до промышленного варианта.

Средняя продолжительность 1 - 2 недели.

Этап 3: развитие прототипа до промышленной экспертной системы

При неудовлетворительном функционировании прототипа эксперт и инженер по знаниям имеют возможность оценить, что именно будет включено в разработку окончательного варианта системы.

Если первоначально выбранные объекты или свойства оказываются неподходящими, их необходимо изменить. Можно сделать оценку общего числа эвристических правил, необходимых для создания окончательного варианта экспертной системы. Иногда при разработке промышленной системы выделяют дополнительные этапы для перехода: демонстрационный прототип - исследовательский прототип - действующий прототип - промышленная система.

Однако чаще реализуется плавный переход от демонстрационного прототипа к промышленной системе, при этом, если программный инструментарий выбран удачно, необязательна перепись другими программными средствами.

Понятие же коммерческой системы в нашей стране входит в понятие промышленный программный продукт, или промышленной экспертной системы в этой работе (табл. 1).

Таблица. 1. Переход от прототипа к промышленной экспертной системе

|  |  |
| --- | --- |
| Демонстрационный прототип ЭС | Система решает часть задач, демонстрируя жизнеспособность подхода (несколько десятков правил или понятий). |
| Исследовательский прототип ЭС | Система решает большинство задач, но не устойчива в работе и не полностью проверена (несколько сотен правил или понятий). |
| Действующий прототип ЭС | Система надёжно решает все задачи на реальных примерах, но для сложной задачи требует много времени и памяти. |
| Промышленная система | Система обеспечивает высокое качество решений при минимизации требуемого времени и памяти; переписывается с использованием более эффективных средств представления знаний. |
| Коммерческая система | Промышленная система, пригодная к продаже, то есть хорошо документирована и снабжена сервисом. |

Основное на третьем этапе заключается в добавлении большого числа дополнительных эвристик. Эти эвристики обычно увеличивают глубинусистемы, обеспечивая большее число правил для трудноуловимых аспектов отдельных случаев. В то же время эксперт и инженер по знаниям могут расширить охват системы, включая правила, управляющие дополнительными подзадачами или дополнительными аспектами экспертной задачи (метазнания).

После установления основной структуры экспертной системы инженер по знаниям приступает к разработке и адаптации интерфейсов, с помощью которых система будет общаться с пользователем и экспертом. Необходимо обратить особое внимание на языковые возможности интерфейсов, их простоту и удобство для управления работой экспертной системой. Система должна обеспечивать пользователю возможность лёгким и естественным образом спрашивать непонятное, приостанавливать работу и т.д. В частности, могут оказаться полезными графические представления.

На этом этапе разработки большинство экспертов узнают достаточно о вводе правил и могут сами вводить в систему новые правила. Таким образом начинается процесс, во время которого инженер по знаниям передаёт право собственности и контроля за системой эксперту для уточнения, детальной разработки и обслуживания.

Этап 4: оценка системы

* После завершения этапа разработки промышленной экспертной системы необходимо провести её тестирование в отношении критериев эффективности. К тестированию широко привлекаются другие эксперты с целью апробирования работоспособности системы на различных примерах. Экспертные системы оцениваются главным образом для того, чтобы проверить точность работы программы и её полезность. Оценку можно проводить, исходяиз различных критериев: критерии пользователей (понятность и «прозрачность» работы системы, удобство интерфейсов и другие.);
* критерии приглашённых экспертов (оценка советов-решений, предлагаемых системой, сравнение её с собственными решениями, оценка подсистемы объяснений и другие.);
* критерии коллектива разработчиков (эффективность реализации, производительность, время отклика, дизайн, широта охвата предметной области, непротиворечивость БЗ, количество тупиковых ситуаций, когда система не может принять решение, анализ чувствительности программы к незначительным изменениям в представлении знаний, весовых коэффициентах, применяемых в механизмах логического вывода, данных и так далее).

Этап 5: стыковка системы

На этом этапе осуществляется стыковка экспертной системы с другими программными средствами в среде, в которой она будет работать, и обучение людей, которых она будет обслуживать. Иногда это означает внесение существенных изменений. Такое изменение требует непременного вмешательства инженера по знаниям или какого-либо другого специалиста, который сможет модифицировать систему. Под стыковкой подразумевается также разработка связей между экспертной системой и средой, в которой она действует.

Когда экспертная система уже готова, инженер по знаниям должен убедиться в том, что эксперты, пользователи и персонал знают, как эксплуатировать и обслуживать её. После передачи им своего опыта в области информационной технологии инженер по знаниям может полностью предоставить её в распоряжение пользователей.

Для подтверждения полезности системы важно предоставить каждому из пользователей возможность поставить перед экспертной системой реальные задачи, а затем проследить, как она выполняет эти задачи. Чтобы система была одобрена, необходимо представить её как помощника, освобождающего пользователей от обременительных задач, а не как средство их замещения.

Стыковка включает обеспечение связи экспертной системы с существующими базами данных и другими системами на предприятии, а также улучшение системных факторов, зависящих от времени, чтобы можно было обеспечить её более эффективную работу и улучшить характеристики её технических средств, если система работает в необычной среде (например, связь с измерительными устройствами).

Пример. Успешно состыкована со своим окружением система PUFF - экспертная система для диагностики заболеваний лёгких. После того, как PUFF была закончена и все были удовлетворены её работой, систему перекодировали с LISP на Бейсик. Затем систему перенесли на ПК, которая уже работала в больнице. В свою очередь, эта ПК была связана с измерительными приборами. Данные с измерительных приборов сразу поступают в ПК. РUFF обрабатывает эти данные и печатает рекомендации для врача. Врач в принципе не взаимодействует с РUFF. Система полностью интегрирована со своим окружением - она представляет собой интеллектуальное расширение аппарата исследования лёгких, который врачи давно используют.

Этап 6: поддержка системы

При перекодировании системы на язык, подобный Си, повышается её быстродействие и увеличивается переносимость, однако гибкость при этом уменьшается. Это приемлемо лишь в том случае, если система сохраняет все знания проблемной области и это знание не будет изменяться в ближайшем будущем. Однако если экспертная система создана именно из-за того, что проблемная область изменяется, то необходимо поддерживать систему в инструментальной среде разработки.

Пример. Примером экспертной системы, внедрённой таким образом, является ХСON (R1) – экспертная система, которую фирма DЕС использует для комплектации ЭВМ семейства VАХ. Одна из ключевых проблем, с которой столкнулась фирма DЕС, - необходимость постоянного внесения изменений для новых версий оборудования, новых спецификаций и так далее. Для этой цели ХСON поддерживается в программной среде ОРS5.

**Тема 5 Современные системы для бизнеса**

**5.1 Развитие компьютерных ИС**

**Историческая справка**

1769-Изобретение парового двигателя Д.Ватт

1776-А.Смит – «История происхождения богатства народов»-принципы разделения труда и

1790-Э.Уитнем предложил использовать сменные части при изготовлении стандартной продукции

1911-Фредерик Тейлор «Принципы научного управления» (деление рабочего процесса на элементы)

Генри Гантт – ученик и последователь Ф.Тейлора, совместно разрабатывали количественные методы организации производства, создатель диаграммы планирования - диаграммы Гантта (Gantt Charts – отражает по горизонтали интервалы времени, а по вертикали - работы, операции, оборудование. ),

Френк и Лилиан Гилбрет (теория устранения непродуктивных движений)

 Генри Форд (создатель сборочного конвейера)

1927- Элтон Мэйо-человеческие отношения в управлении производством

Абрахам Маслоу, Фредерик Херцберг, Дуглас Мак-Грегор, Уильям Оучи – различные теории мотивации

**Великие научные открытия**

**-научное управление**

разработка математических методов решения производственных проблем

**-революция качества**

 применение новых методов **JIT**, **TQM**

**-информационные технологии**

 интегрированное компьютерное производство, гибкие производственные системы, появление **WWW**

**-глобализация**

рост масштабов торговли, транснациональные корпорации, страновая конкурентная борьба

* 40-е- исследование возможностей ЭВМ по переработке экономической информации.
* 50-е-применение компьютеров в управлении производством (Впервые в 1954г. компанией General Electric).
* 60-е-методы совершенствования систем принятия решений (линейного программирования, теории расписаний, управления проектами).Исследования по архитектуре СУБД, первые пакеты прикладных программ.
* 70-е-создана система экономико-математических методов исследования разработана и воплощена концепция производственных ИС: MRP-Material Requirements Planning, MRPII-Manufacturing Resource Planning. Созданы ПЭВМ.
* 80-е-проблема создания CIM-Computer Integrated Manufacturing. Использование ERP-Enterprise Resource Planning и их интеграция с системами CAD/CAM - Computer Aided Design/Manufacturing
* 90-е-развитие систем принятия решений, экспертных систем, систем искусственного интеллекта. Внедрение комплексных решений на основе локальных сетей. Мощных СУБД, новых технологий проектирования.

**5.2 Классификация ИС**

*По степени уникальности*

* Заказные (уникальные) системы, разработка которых относится к НИОКР
* Адаптируемые системы – приспосабливаемые на конкретном предприятии готовые решения ИС

*По масштабу системы*

* Системы начального уровня –т.н. коробочные или low end (количество пользователей – от одного до нескольких десятков сотрудников; могут работать на отдельных компьютерах или в небольшой сти не очень требовательны к выделяемым ресурсам; могут устанавливаться самостоятельно, не требуют сложных настроек; работают локально, но могут стыковаться с др. программными продуктами)
* Среднего класса - middle end (больший объем функций, более высокая стоимость (от нескольких сотен до десятков тысяч долларов), как правило являются учетными системами с усеченным функционалом для средних и крупных предприятий со значительным количеством пользователей, требуют специальной настройки и обучении пользователей, услуги по внедрению могут включать анализ деятельности предприятия и адаптацию, инсталляцию и настройку системы, обучение пользователей, сервисное обслуживание на определенный срок; в основном это российские учетные системы, занимающие промежуточное положение между коробочными и системами высшего класса)
* Высшего класса – high end (высокий и даже избыточный уровень детализации бизнес-процессов, охватывают управление всеми ресурсами предприятия, высокие затраты на внедрение – больше стоимости лицензий в сотни раз, т.к. требуется длительный срок внедрения и наличие на предприятии подразделения специалистов, которые должны осуществлять перенастройку системы в соответствии с изменениями бизнеса и интеграцию с другими имеющимися системами . При внедрении как правило требуется реорганизация бизнес-процессов. Класс не ниже ERP).

*По уровню исполнения*

* АСУ цехом
* АСУ производством
* АСУ отрасли

*По типу производства*

* АСУ дискретным производством
* АСУ непрерывным производством
* АСУ дискретно-непрерывным производством

*По типу принимаемого решения*

* Информационно-справочные
* СППР (экспертные)
* Информационно-управляющие (роботы, оборудование с ЧПУ, АСУТП)

*По назначению*

* Военные
* Экономические
* ИС менеджмента
* Информационно-поисковые

По областям деятельности

* Медицинские
* ТЭК
* Экологические
* Геоинформационные
* Мн. Др.

***Современные системы для решения бизнес - задач***

* ***PDM – Product Data Management*** – система управления данными об изделии
* ***CRM - Customer Relationship Management*** – система управления взаимоотношениями с клиентами
* ***SCM – Supply Chain Management*** – система управления поставками
* ***ERP – Enterprise Resource Planning*** – система управления ресурсами предприятия
* ***PLM – Product Lifecycle Planning*** – система управления жизненным циклом изделия

***Связь ИС с жизненным циклом изделия***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Исследование | Разработка | Подготовка | Производство | Ликвидация |
|   |   |   |   |   |

***Возрастание роли стратегического управления***

Стратегическое управление – цепь, состоящая из 4-х ключевых звеньев:

* Стратегическая диагностика (точный диагноз финансово-экономического состояния предприятия и его положения на рынке)
* Выбор стратегических целей (компромисс возможностей и ограничений, анализ стратегических альтернатив, оценка выгод и рисков)
* Стратегическое планирование (разрыв между состоянием «как есть» и «как будет» заполняется проектами, приближающими компанию к намеченной цели)
* Стратегический контроллинг (менеджеры должны иметь возможность отслеживать процессы выполнения стратегии и оперативно корректировать стратегические планы)

***Самые известные Российские аналитические системы***

* АБФИ (компания ЛАНИТ (Вестона)) – Универсальная система для решения прикладных задач финансового анализа, включающая три модуля: АБФИ-банк, АБФИ-предприятие, АБФИ-страховая организация.
* АК «Прогноз» (комп. Прогноз) – аналитический комплекс, включающий функции сбора, обработки и анализа экономических показателей предприятия и выработки стратегий развития.

***Компания Про- Инвест***

* Audit Expert – Анализ финансового состояния предприятия.
* ***Project Expert*** – Разработка планов развития бизнеса, анализ рисков и эффективности бизнес-моделей
* Marketing Expert – Планирование и анализ корпоративного маркетинга, оценка положения компании на рынке, анализ и формирование оптимальной структуры сбыта
* Sales Expert – Оптимизация работы с продажами и организации работы с клиентами.
* Forecast Expert – Прогнозирование процессов и факторов развития редприятия за счет анализа экономических показателей и тенденций развития рынка, предопределение спроса на продукцию и услуги компании, будущих объемов реализации, курсов валют, фьючерсов, акций и др.
* Invest Center – Настраиваемая ИС финансового мониторинга и планирования деятельности предприятий и региональных экономических объединений
* Client Center – Разработанная совместно с WinPeak International настраиваемая CRM-система для автоматизации работы отделов маркетинга, сбыта и сервисного обслуживания.

***ИНЭК***

* ИНЭК – Аналитик – Стратегическое планирование, оценка и разработка инвестиционных проектов
* ИНЭК – Холдинг – Оценка и прогнозирование финансового состояния группы предприятий и планирование их финансово-хозяйственной деятельности
* ИНЭК – АФСКБ – Анализ финансового состояния коммерческих банков.
* ИНЭК – АФСП/ ИНЭК – АДП - Диагностика, оценка и мониторинг финансово-хозяйственного состояния предприятия.

***Компания Курс – Marketing Analytic 5. Модули:***

* C-Commerce – CRM-система для сбора информации о клиентах, автоматизации работы,SWOT анализ и нализ привлекательности.
* Analyzer – система автоматизации маркетинговых исследований и анализа внутренних данных о рыночной деятельности предприятия и его конкурентов.
* Geo – инструмент визуализации маршрутизации данных на географических картах
* Predictor – система микроэкономического анализа и прогнозирования маркетинговой деятельности.
* Conjoint- система анализа и оптимизации потребительских свойств продукции
* Portfolio- система обработки результатов экспертных исслкдований рынка и подготовки предложений для решений стратегического маркетинга

***Компания Альт***

* Альт- форм – Методические материалы для подготовки бизнес-планов
* Альт- инвест – Разработка инвестиционных пректов
* Альт- лизинг – Расчет и оптимизация графика платежей по условиям лизинга
* Альт-финансы – Анализ и прогнозирование экономических показателей предприятия
* Альт- прогнозы – Диагностика, оценка и прогнозирование состояния и перспектив деятельности предприятия
* Корпоративные финансы (Компания Инталев) – анализ финансового состояния предприятия и разработка плановых предложений по повышению эффективности его работы.
* ***Deductor*** (компания BaseGroup Labs) аналитическая программа, основанная на использовании OLAP, KDD, Data Mining решений и инструментов, располагающая широким спектром отлаженных аналитических технологий, применяемых для решения большого спектра бизнес-задач.

***Самые известные зарубежные аналитические системы***

* Marketing Optimization (SAS, США) – Дополнение к технологиям автоматизации маркетинга и управления маркетинговыми кампаниями, позволяющее планировать и ранжировать по приоритетности все исходящие потоки коммуникаций.
* Oros Analytics (ABC Technologies Inc., США) – обработка данных, поступающих из ERP и CRM систем и их консолидация. Принятие тактических и стратегических решений на основе обобщенной модели.
* Alcar Strategic Financial Planning Systems (Alcar Group Inc. США) – Редактируемая финансовая модель для каждого подразделения компании и дочерних структур. Консолидация финансовой информации. Принятие тактических и стратегических решений на основе обобщенной модели.
* Business Insight (Business Resource Software Inc., США) – Автоматизированный анализ деятельности предприятия и его положения на рынке, базирующийся на основании анкеты пользователей. Рекомендации по поводу стратегии.
* ABC Focus (Cash Focus Pty Ltd, Австралия) – Система расчета актуальной себестоимости продуктов и услуг.
* Marketing Plus (Computer Corp. of America, США) – Поэтапное построение плана маркетинга на основании миссии, целей и стратегии компании. Анализ расхождения план-факт.
* ABM Tools (Decimal Technologies Inc., США) – Перевод данных, поступающих из ERP систем на язык Activity-Based Cosing и анализ издержек по финансовой модели предприятия.
* Ithinc (High Performance Systems, США) – Построение и анализ имитационных бизнес-моделей.

**EDEMS - Автоматизированные технологии работы с документами**

***Компании, создающие данные продукты (EDEMS) :***

* Термика ([www.termica.ru](http://www.termica.ru/))
* Электронные офисные системы ([www.eos.ru](http://www.eos.ru/))
* IRP Technology ([www.irptec.ru](http://www.irptec.ru/%22%20%5Ct%20%22_parent))
* Интер Траст ([www.intertrast.ru](http://www.intertrast.ru/))
* ОСГ Рекордс Менеджмент ([www.osgrm.com](http://www.osgrm.com))

***EDEMS***

* **Directum, Директум** ([www.directum.ru](http://www.directum.ru/%22%20%5Ct%20%22_parent), [www.npo-comp.ru](http://www.npo-comp.ru/%22%20%5Ct%20%22_parent))
* БОСС-Референт, АйТи ([www.it.ru](http://www.it.ru/))
* Евфрат-документооборот, Cognitive technologies (www.evfrat.ru)
* Промтара ПКФ ([www.promtara.com](http://www.promtara.com/))
* DocsVision ([www.docsvision.com](http://www.docsvision.com/))
* NAUMEN ([www.naumen.ru](http://www.naumen.ru/))
* Дело, электронные офисные системы (www.eos.ru)
* Золушка, НТЦ ИРМ ([www.mdi.ru](http://www.mdi.ru))
* Экстракод ([www.extracode.ru](http://www.extracode.ru/),
* [www.s-q.ru](http://www.s-q.ru/))
* НойХаусГрупп ([www.neuhaus.ru](http://www.neuhaus.ru/))
* Триал электроникс ПДС ([www.trialelectronics.ru](http://www.trialelectronics.ru/))
* Электронный архив ([www.elar.ru](http://www.elar.ru/))
* Интерпроком Лан ([www.interprocom.ru](http://www.interprocom.ru/))
* СофтИнформ ([www.softinform.com](http://www.softinform.com/))
* PayBot ([www.paudox.ru](http://www.neuhaus.ru/%22%20%5Ct%20%22_parent), [www.paubot.com](http://www.paubot.com/%22%20%5Ct%20%22_parent))
* Документум

***Инструменты для эффективного управления дискуссиями***

* Microsoft Office Live Meeting – приложение для проведения Web-конференций
* WebEX от компании WebEX Communication – приложение для проведения Web-конференций
* Thin Tank компании Group Systems – проведение онлайн заседаний, согласно повестки дня, принятие решений методом «мозгового штурма». ([www.groupsystems.com](http://www.groupsystems.com/))
* Super Decisions (Creative Decisions Foundations) Инструмент поддержки принятия решений на основе аналитической методологии Analytic Network Process, разработанной Томасом Саати ([www.superdecisions.com](http://www.superdecisions.com/%22%20%5Ct%20%22_parent))
* Expert Choice11 (Expert Choice) – ПО для поддержки принятия коллективных решений, в котором используется аналитический иерархический процесс (Analytic Hierarchy Process) ([www.expertchoice.com](http://www.expertchoice.com/))
* Imaginatic Idea Central (Imaginatic) Web – приложение для управления сбором, ранжированием и реализацией идей, а также для оценки вклада каждого участника обсуждения (www.imaginatic [.com](http://www.ce.com/%22%20%5Ct%20%22_parent))

***Управление персоналом- Базовые, рекрутинг, управление поощрениями, оценка эффективности сотрудников, планирование рабочих смен***

* Oracle (Enterprise HCM suite)
* SAP (HCM)
* Lawson (Human Capital Management)
* Kronos Workforce (HR Emploee Manager)
* 1С:УПП 8 (1С:Зарплата и управление персоналом 8, подсистема Управление персоналом)

*Электронный рекрутинг*

* Kronos Workforce (Acquisition)
* Peopleclick (Requirements Management)
* Taleo (Enterprise Staffing Management)

*Управление поощрениями*

* 1С:УПП 8 (1С:Зарплата и управление персоналом 8, подсистема Управление персоналом)
* Synygy (EIM)
* Callidus (TrueComp)
* Authoria (Compensation Advisor)

*Оценка эффективности сотрудников*

* 1С:УПП 8 (1С:Зарплата и управление персоналом 8, подсистема Управление персоналом)
* Kenexa (Career Tracker)
* Witness Systems (eQuality Contact Store)
* SHL (Group Obgective Assesment)

*Планирование рабочих смен и нагрузки*

* 1С:УПП 8 (подсистема Управление производством)
* Kronos Workforce (Ctntral)
* Eclipsys (Sunrise Enterprise Scheduling)
* Workbrain (Enterprise Workforce Management)
* Witness Systems (Enterprise Activity Manager, Advisor Express)

*Расчет заработной платы*

* 1С:УПП 8 (1С:Зарплата и управление персоналом 8, подсистема Расчет заработной платы)
* Oracle (Enterprise HCM, Global Payroll)
* CBS (Payroll for Intuit)
* Ultimate (UltiPro Pauroll Administration and Tax Management)

**ERP**

***ERP – Enterprise Resource Planning***

***ИС управления предприятием***

***Хаотичная автоматизация***

* Отсутствие стратегического плана
* Неправильное понимание роли и функций отдела АСУ, ИТ
* Решение локальных задач
* Критерии: уровень знаний, возможность получить эксклюзивные скидки на ПО
* Результат: - дорогая интеграция

 - дублирование функций

Автоматизация по участкам

* Автоматизация отдельных подразделений, объединенных по функциональному признаку (бухгалтерия, участок сортировки и др.)
* Если недостаточны инвестиционные ресурсы предприятия
* Если существуют участки, где применение ИС дает существенное увеличение производительности
* Если технология или иное не позволяют обходиться без автоматизации
* Основное средство – специализированные АСУТП
* Для эффективности подхода необходимы корректируемые стратегический и оперативный планы автоматизации

 Автоматизация по направлениям

* Автоматизация отдельных направлений (производство, сбыт, управление финансами)
* Использование систем класса MRP,MRPII,ERP
* Предполагает участие всех подразделений (от производственных до управленческих, напр., снабжение)
* Создание телекоммуникационной структуры предприятия
* Связана с реинжинирингом бизнес-процессов, требует создания модели предприятия
* Требует корректируемых стратегических планов после окончания автоматизации направления

 

Полная автоматизация

* ERP-иерархические структуры, состоящие из элементарных управленческих процедур, включаемых в АСУП
* АСУП как система состоит из подсистем, блоков управления, модулей, управленческих функций, операций.
* Интеграция проявляется во всех функциональных и обеспечивающих подсистемах
* Предполагается такое объединение и согласование управленческих функций, чтобы в ходе процесса управления предприятием обеспечивалась его оптимизация
* Результат – единый стандарт и функциональная интеграция (CAD+CAM=CIM)

Ориентация ERP на управление производственным процессом

циклом изделия

процессами, обеспечивающая непрерывность

Комплексное решение для управления бизнесом

Миссия ERP – систем

**Система управления бизнесом – это больше, чем просто одна из программ – это стратегия и методология, которые необходимо внедрить в вашу компанию.**

Стратегия при поддержке ИС позволит вам

* *повысить качество производства*,
* *качество обслуживания клиентов*,
* *повысить эффективность и прибыльность бизнеса*

Текущие задачи ***ERP***

* Сегодня система управления предприятием рассматривается как инструмент для реформирования организации в целом, реинжиниринга ее бизнес-процессов.
* Руководству компаний нужны новые технологии управления, которые в то же время позволяют учесть управленческий опыт предприятия, особенности бизнес-среды.
* Для выхода на международный рынок публичных заимствований требуется система, имеющая широкое распространение в мире и известная инвесторам и аудиторам.
* Желательны готовые отраслевые решения для мобильного внедрения, либо интеграция с другими менеджерскими IT-решениями (например с PDM в машиностроении).

Текущие задачи ***ERP***

* В ближайшее время на предприятиях ERP-системы первого поколения, отработавшие 10-12 лет, будут активно заменяться современными версиями.
* Это повлечет за собой смену методов планирования и управления предприятием (с MRP,MRPII – APS (Advanced Planning & Scheduling) – системы расширенного производственного планирования и SCM).
* Изменится архитектура ИС с вертикально-ориентированной модели объектов данных CIM на совмещенные вертикально-горизонтальные SCOR, REPAC.
* В ближайшем будущем должны появиться универсальные языки обмена данными о производственных системах для интеграции с внешней средой, клиентами, чтобы не зависеть от типа их системы.

***Развитие современных программ ERР – класса***

* SAP/R3 (SAP Business One ) от компании SAP (Systems, Applications and Products in Data Processing).
* Oracle Applications от корпорации Oracle
* Baan IV (Baan ERP) от компании Baan
* Renaissance Cs от компании Ross Systems
* Microsoft Business Solution от Microsoft, Microsoft Dynamics AX
* Босс Корпорация от компании Ай Ти

Средняя стоимость ERP – системы

* Стоимость складывается из ***цены покупаемых лицензий*** и ***цены консалтинговых услуг по внедрению проекта***
* Усредненная стоимость одной лицензии сегодня стоит от 2 до 4тыс. евро
* Стоимость всего ERP-проекта от 200 до 350тыс. евро

**R3 от SAP AG**

В 1972г. в Германии пять инженеров образовали маленькую фирму с громким названием

 ***Systemanalyse und Programmentwicklung.***

Они решили создать универсальное программное обеспечение для решения организационно-экономических задач предприятия.

В настоящее время компания называется ***SAP: Systems, Applications and Products in Data Processing***

**SAP – лидер поставок интегрированных КИС**

Программный продукт объединяет все хозяйственные процессы предприятия, разработаны две линии развития продукта:

* **Система SAP/R2** для суперкомпьютеров
* **Система SAP/R3** для конфигураций клиент/сервер. **Основные характеристики:**
* *модульные структуры;*
* *общее хранение данных;*
* *открытость;*
* *международный характер;*
* *возможность применения для любой отрасли.*
* *интеграция приложений;*

**Основные достижения**

* В компании работает свыше 17000 сотрудников
* Офисы компании расположены в более 50 странах мира
* **В СНГ SAP работает с 1992г.**
* В РФ продукт применяют представительства Mars, Colgate, Reebok, РАО «ЕЭС», Туламашзавод, Донецкий металлургический, Омский НПЗ, Чепецкий металлургический
* По итогам 2006г. Россия и СНГ вышли на второе место в регионе ЕМЕА по объему продаж лицензий SAP, уступив только Британии.

Основные модули системы ***SAP***

* Финансовая бухгалтерия (FI)
* Контроллинг (CO)
* Управление материальными потоками (ММ)
* Техническое обслуживание и ремонт оборудования (PM)
* Продажи, отгрузка, фактурирование (SD)
* Система проектов (PS)
* Управление, планирование и контроль основных средств (AM)
* Управление персоналом (HR)

**Oracle Applications от Oracle**

* Корпорация Oracle была основана в Калифорнии (США) в 1977г.
* Является крупнейшим в мире поставщиком СУБД, второй в мире компанией на рынке программного обеспечения (после Microsoft), занимает второе место по поставкам КИС «Oracle Applications»
* Количество сотрудников по всему миру превышает 25тыс.
* Установлены продукты в РФ – Ростелеком, химические, нефтехимические предприятия (Татарстан, Уральский федеральный округ), металлургия (Магнитка), Внешэкономбанк

**Основные модули системы Oracle**

* Управление финансами
* Управление материальными потоками
* Управление производством
* Управление проектами
* Управление персоналом
* Управление маркетингом

**Специализация Oracle – продукты для банковской сферы**

* CRM - система
* Customer Data Hub – центр данных о клиентах
* Oracle Financial Services Applications (OFSA) – приложения для финансовых структур (используется в более, чем 250 финансовых институтах)
* Oracle Risk Manager – управление рисками
* Оracle Transfer Pricing – обеспечивает формирование трансфертных цен для внутрибанковских расчетов
* Financials – внутрихозяйственная бухгалтерия
* HR – управление кадрами
* i-Learning – дистанционное обучение сотрудников (первые среди компаний-поставщиков ПО начали интерактивно обучать пользователей через Интернет)
* Internal Controls Manager – внутренний аудит

**Система Renaissance CS от компании Ross Systems**

* Компания **Ross Systems была основана в 1972г. И акционирована в 1991г.**
* **Штаб-квартира находится в Атланте (США)**
* **Имеет более 50 филиалов во всем мире**
* **В компании работает более 600 сотрудников**
* **Основной продукт - КИС Renaissance CS, ранее известная как PROMIX, инсталлирована более чем на 3000 предприятиях в 60 странах мира на 16 различных языках**
* **В РФ с 1998г., основное применение в российских филиалах транснациональных компаний**

***Отраслевые решения Renaissance CS***

* Ориентация на предприятия, технологические процессы которых описываются с помощью формул, спецификаций и рецептур
* Внедряется на предприятиях химической, продовольственной, фармацевтической, целлюлозно-бумажной, металлургической и др. отраслей промышленности. Есть примеры внедрения в здравоохранении.

Российские комплексные бизнес - решения

**Система управления БОСС компании АйТи**

* Компания работает на отечественном рынке с 1990г.
* В основных подразделениях работает свыше 600 сотрудников
* Основные подразделения находятся в Москве, Санкт - Петербурге, Уфе, Казани, Волгограде, Красноярске, Иркутске

**Функциональные возможности
КИС БОСС**

Охватывают все основные бизнес-процессы как государственной бюджетной организации, так и коммерческого предприятия:

* Управленческий и бухгалтерский учет
* Финансовый менеджмент
* Управление персоналом
* Логистика
* Маркетинг и продажи
* Управление производством
* Информационно - защищенное делопроизводство и документооборот

БОСС – Корпорация

Полномасштабная система управления финансово-хозяйственной деятельностью, разработанная для крупных корпораций со сложной структурой.

**Включает в себя бизнес-приложения:**

* **БОСС-Компания**
* **БОСС-Кадровик**
* **БОСС-Референт**
* **БОСС-Архив**
* **БОСС-Коммерсант**
* **БОСС-Аналитик**

**Тема 5 Корпоративные информационные системы**

1. **Понятие КИС**

*Корпоративной информационной системой* (КИС) принято называть совокупность специализированного программного обеспечения и вычислительной аппаратной части, реализующую некоторый набор средств, автоматизирующих отдельные функции управления предприятием. Под этими функциями, как правило, понимается управление бизнес-процессами предприятия таким образом, чтобы увязать деятельность отдельных подразделений с движением финансовых и товарных потоков по всей технологической цепочке управленческих процедур.

Как следует из данного определения, корпоративная информационная система всегда существует в контексте некоторого конкретного *бизнес-процесса* предприятия. Под бизнес-процессом обычно принято понимать общую модель деятельности предприятия, выраженную в терминах внутренних и внешних связей. В рамках бизнес-процесса отображаются все объекты (сущности), процессы, правила выполнения операций, существующая стратегия развития, а также критерии оценки эффективности функционирования системы. Форма представления бизнес-процесса и уровень её детализации определяются целями моделирования и принятой точкой зрения.

Основой концепции современных КИС является схема, включающая комплексное управление финансовыми и товарными потоками, себестоимостью продукции и персоналом предприятия в разрезе этапов стратегического и оперативного планирования, управленческого и оперативного учета с выходом на бухгалтерский учет. *Управление* финансовыми потоками *в стратегическом плане* - это планирование доходов и расходов по разным периодам, планирование получения, распределения и поглощения привлеченных средств с учетом влияния внешних параметров (уровня инфляции, курсов валют, стоимости кредитов, ставки рефинансирования и т.д). *Оперативное планирование* представляет собой формирование совокупности финансовых планов и бюджетирования направлений деятельности. На этапе стратегического планирования управление товарными потоками представляет собой план выпуска и сбыта продукции для производственного предприятия или маркетинговый план закупок и продаж для оптовых торговых фирм. На уровне оперативного планирования товарных потоков концепция предусматривает увязку заключения договоров на поставку с планами запуска производства или осуществления закупок на основе системы календарей движения товарных и финансовых потоков. При этом товарные потоки рассматриваются с позиции всех точек продвижения, что позволяет моделировать любые схемы хозяйственной деятельности, вплоть до многоходовых бартерных сделок и оперативного управления движением по складам.

*Основное назначение корпоративных информационных систем* - оперативное предоставление непротиворечивой, достоверной и структурированной информации для принятия управленческих решений. Такие системы образуют единое информационное пространство всей деятельности предприятия, которая обеспечивается соответствующими его подразделениями или отдельными людьми, выполняющими определенные функции. В их числе - финансовый отдел, сбыт и снабжение, обслуживание клиентов, складское хозяйство и логистика; производственные подразделения. Часто к ним добавляются отделы кадров, планово-экономические и договорные службы предприятия, делопроизводство, бухгалтерия и т.д. Наличие в корпоративных системах управления встроенных средств и механизмов позволяет персонифицировано контролировать выполняемые операции, а также осуществлять доступ к информации и ее использование.

Основные задачи, выполняемые КИС в разрезе понятий стратегического и оперативного планирования, оперативного и бухгалтерского учёта, можно представить следующей таблицей.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  ФункцииЭтапы | Управление финансовыми потоками | Управление товарными потоками | Управление себестоимостью | Управление персоналом |
| Стратегическоепланирование | Финансовое планирование, бюджетирование | Товарный план закупок и продаж | Бизнес-планирование | Бизнес-планирование |
| Оперативноепланирование | Финансовое планирование по контрактам | Товарный календарь по контрактам | Технико-экономическое планирование | Персонификация деятельности по исполнителям |
| Оперативный учёт | Исполнение финансовой части контрактов | Исполнение товарной части контрактов | Мониторинг себестоимости | Табельный учёт, наряды, учёт контрактов |
| Бухгалтерскийучёт | Бухгалтерское разделение финансов | Материальный учёт | Учёт фактических затрат | Расчет заработной платы |

Механизмы и особенности выполнения перечисленных задач зависят от модели бизнес-процесса, принятого на конкретном предприятии. Внедрение КИС имеет целью не только автоматизацию деятельности предприятия, но и изменение способа ведения дел, его модернизацию. В процессе внедрения КИС вся организация приобретает новое понимание своего бизнеса и отношение к нему.

Несмотря на различие моделей бизнес-процесса на различных предприятиях понятие КИС несёт в себе и ряд универсальных аспектов. Их легко понять, рассмотрев нижеследующие разделы данной лекции.

*Отличие КИС от ERP*

ERP-система – это обязательно КИС. КИС может не быть ERP-системой.

MRP (Material Requirements Planning)

CRP (Capacity Resources Planning)

MRPII (Manufacturing Resources Planning)

ERP (Enterprise Resources Planning) и др.

* заимствованы из американского лексикона
* отражают некие концепции, которые могут применяться при создании той или иной КИС

*Что дает внедрение КИС?*

* Снижение транспортно-заготовительных расходов на 60%
* Сокращение производственного цикла по заказным изделиям на 50%
* Сокращение количества задержек с отгрузкой готовой продукции на 45%
* Уменьшение уровня неснижаемых остатков на складах на 40%
* Снижение производственного брака на 35%
* Уменьшение административно-управленческих расходов на 30%
* Сокращение производственного цикла по базовым изделиям на 30%
* Уменьшение складских площадей на 25%
* Увеличение оборачиваемости средств в расчетах на 30%
* Увеличение оборачиваемости ТМЗ на 65%
* Увеличение количества поставок точно в срок на 80%

MPS (Master Planning Shedule) – методология «объемно-календарного планирования»

* является базовой практически для всех планово-ориентированных методологий
* применяется в основном в производстве
* может использоваться и в других отраслях бизнеса (например, дистрибуции)

MRP (Material Requirements Planning) – методология планирования потребности в материальных ресурсах

* определяет конечную потребность в ресурсах по данным объемно-календарного плана производства
* ключевое понятие «разузлование» (приведение древовидного состава изделия к линейному списку (Bill of Materials), по которому планируется потребность и осуществляется заказ комплектующих)

CRP (Capacity Requirements Planning) – планирование производственных ресурсов

* CRP применяется совместно с MRP (ввиду тесной логической связи при планировании)
* методологии MRP/CRP применяются в АСУП производственных мероприятий
* Отличие от MRP:
	+ вместо единого понятия состава изделия использует понятия: «обрабатывающий центр», «машина», «рабочие ресурсы», ввиду чего технически реализация CRP более сложна

MRPII (Manufacturing Resource Planning) – планирование производства

* интегрированная методология, включающая MRP/CRP и, как правило, MPS и FRP
* при использовании данной методологии обязательно подразумевается анализ финансовых результатов производственного плана

FRP (Finance Requirements Planning) – планирование финансовых ресурсов

ERP (Enterprise Resources Planning) – концепция бизнес-планирования

* под ERP подразумевается «интегрированная» система, выполняющая функции, предусмотренные концепциями MPS-MRP/CRP-FRP
* Отличия от MRPII:
	+ ERP имеет возможность «динамического анализа» и «динамического изменения плана» по всей цепочке планирования
	+ конкретные возможности методологии ERP существенно зависят от программной реализации
	+ концепция ERP более «размыта», чем MRPII
	+ методология ERP оказывается применимой и в торговле, и в сфере услуг, и в финансовой сфере. MRPII имеет явно выраженную направленность на производственные компании

CSRP (Customer Synchronized Resources Planning) – планирование ресурсов, синхронизированное с покупателем

* CSRP включает в себя полный цикл – от проектирования будущего изделия с учетом требований заказчика, до гарантийного и сервисного обслуживания после продажи
* CSRP интегрирует покупателя в систему управления предприятием (т.е. не отдел продаж, а сам покупатель размещает заказ на изготовление продукции, сам отвечает за правильность его исполнения и при необходимости отслеживает соблюдение сроков производства и поставки)
* Предприятие может очень четко отслеживать тенденции спроса на свою продукцию

SCM (Supply Chain Management) – управление цепочками поставок

* оптимизирует управление логистическими цепями
* позволяет существенно снизить транспортные и операционные расходы путем оптимального структурирования логистических схем поставок
* концепция SCM поддерживается в большинстве систем ERP- и MRPII-класса

CRM (Customer Relationship Management) – концепция построения автоматизированных систем обслуживания клиентов компании

* CRM подразумевает накопление, обработку и анализ не только финансово-бухгалтерской, но и прочей информации о взаимоотношениях с клиентами
* способствует повышению производительности менеджеров, улучшает качество обслуживания клиентов и способствует увеличению продаж

ВЫВОД: изучайте, как в системе реализованы конкретные функции, как осуществляются важные для Вашей компании процессы. Так меньше шансов купить «куклу».

**Классификация КИС**

1. **Локальные системы**
* предназначены для автоматизации учета по одному или нескольким направлениям (бухгалтерия, сбыт, учет кадров)
* может воспользоваться практически любое предприятие, нуждающееся в управлении финансовыми потоками и в автоматизации учетных функций
* универсальны (но ряд разработчиков предлагает отраслевые решения, например, особые способы начисления налогов и т.п.)
* цикл внедрения локальных систем невелик, иногда можно воспользоваться «коробочным» вариантом, купив программу и самостоятельно развернув ее на предприятии
* стоимость локальных систем колеблется в диапазоне $5 000 – $50 000
1. Финансово-управленческие системы
* гибко настраиваются на нужды конкретного предприятия
* хорошо интегрируют деятельность предприятия
* предназначены для учета и управления ресурсами непроизводственных компаний
* универсальны, однако необходимо более четко отражать специфику деятельности предприятия
* функциональные возможности шире, чем у локальных
* во многих системах данного класса присутствуют базовые возможности управления производством
* стоимость финансово-управленческих систем можно условно определить в диапазоне от $50 00 до $200 000
1. Средние интегрированные системы
* предназначены для управлением производственным предприятием и интегрированного планирования производственного процесса
* учетные функции проработаны глубоко, но выполняют вспомогательную роль
* порой невозможно выделить модуль бухгалтерского учета: информацию в бухгалтерию поступает автоматически из других модулей
* цепочка планирования «сбыт – производство – закупки» на основе процедур MRPII является ядром этих систем
* подразделения предприятия (финансы, бухгалтерия, маркетинг и пр.) строят свою деятельность, опираясь на данные этой цепочки
* значительно сложнее в установке: цикл внедрения занимает от 6 месяцев до полутора лет и более
* система покрывает потребности подразделений и полностью интегрирует производственное предприятие, что требует значительных совместных усилий сотрудников предприятия, поставщика КИС или консалтинговой компании, осуществляющей внедрение
* по многим параметрам значительно жестче, чем финансово-управленческие
* производственное предприятие должно работать, как хорошо отлаженные часы, где основными механизмами управления являются планирование и оптимальное управление запасами и производственным процессом, а не учет количества счетов-фактур за период
* стоимость внедрения средних систем $50 000 - $500 000 и более
1. Крупные интегрированные системы
* сходные функции присутствуют и во многих финансово-управленческих (за исключением производства) и средних интегрированных системах, однако с более низкой степенью проработки
* отличаются от средних набором вертикальных рынков и глубиной поддержки процессов управления большими многофункциональными группами предприятий (холдингов или ФПГ)
* имеют наибольшую функциональность (включая управление производством, управление сложными финансовыми потоками, корпоративную консолидацию, глобальное планирование и бюджетирование и пр.)
* сроки внедрения крупных интегрированных систем обычно занимают более года
* стоимость проекта более $500 000

Отказываемся от КИС?

Условия:

* вы в одиночку или с партерами лично контролируете весь Ваш бизнес
* папки с обрабатываемыми за год документами помещаются на рабочем столе
* в вашей голове умещаются все поставщики, покупатели и сотрудники, а также заказы, заявления, приказы, суммы долга

Итог:

* вы – менеджер малого предприятия

КИС нужна, когда:

* с Вами здоровается сотрудник, фамилию которого Вы не знаете
* в компании много людей, которых принимали на работу не Вы
* в бухгалтерии несколько шкафов с бумагами; столько же в отделе сбыта, и это несмотря на то, что часть уже переместили в архив
* Вам приносят ведомость безнадежных долгов покупателей
* Вам звонит разъяренный заказчик и требует объяснений
* Вы не в состоянии управлять компанией так, как раньше
* Ваша компания превратилась в СЛОЖНУЮ СИСТЕМУ

Подумать о покупке КИС нужно не дожидаясь негативных последствий дезорганизации в управлении компанией.

Стоимость проекта:

* *стоимость компьютерной техники и коммуникационного оборудования*
* *стоимость лицензии на использование КИС*
* *стоимость системного программного обеспечения и сервера баз данных (СУБД)*
* *стоимость обследования и проектирования*
* *стоимость внедрения КИС*
* *стоимость эксплуатации КИС*

Совокупная стоимость КИС:

1. стоимость оборудования информационной системы и системного ПО
2. стоимость лицензии на использование КИС
3. стоимость обследования, проектных и внедренческих работ

Совокупные затраты распределяются: 1:1:3 – 1:1:5

Техническая составляющая не потребуется, если:

* в компании уже имеется развитая компьютерная инфраструктура

Техническая составляющая потребуется, если:

* придется увеличить мощность сервера, или приобрести новый
* предприятие имеет территориально-распределенную структуру (придется приобретать выделенные каналы связи для обеспечения информационного обмена)

Стоимость лицензий на использование КИС формируется по-разному:

* лицензия на одного так называемого «конкурентного пользователя»
* самая распространенная схема лицензирования – «конкурентный пользователь модуля»
* серверная лицензия (лицензия на систему в целом или серверная лицензия на конкретный модуль)

Вывод: внимательно анализируйте лицензионную политику поставщиков КИС, за кажущейся дешевизной могут скрываться неприятные сюрпризы

Стоимость системного программного обеспечения и СУБД:

* промышленные СУБД (например Oracle, MS SQL Server, Informix, Unify) стоят весьма недешево
* все фундаментальные КИС имеют в своем фундаменте серьезную СУБД
* только СУБД промышленного класса сможет обеспечить надежное хранение деловой информации и быструю обработку данных
* рассматривая вопрос о приобретении КИС, обязательно поинтересуйтесь у поставщика КИС – она может кардинально отличаться от лицензионной политики поставщика КИС

Стоимость обследования, проектирования и внедрения КИС:

* стоимость проектирования составляет наиболее ощутимую часть от совокупных затрат
* стоимость внедрения прямо зависит от сложности структуры компании и автоматизируемых процессов, от потребности в заказной настройке (доработке) КИС
* затраты чаще всего превышают общую стоимость программного обеспечения
* особенно дорого стоит внедрение зарубежных КИС, затраты на внедрение которых могут в 4-5 раз превышать стоимость лицензий

*Купить или разрабатывать своими силами?*

На разработку КИС фирмы-разработчики затрачивают сотни, а то и тысячи человеко-лет, а бюджеты проектов создания систем даже у российских разработчиков измеряются миллионами долларов.

Будет ли КИС документирована так, что после того, как Ваши программисты по каким-либо причинам покинут компанию, новые смогут разобраться в системе и продолжить ее сопровождение и развитие?

*Целесообразность разработки КИС своими силами?*

Разрабатывать своими силами стоит, если Вы:

* ставите задачу на разработку коммерческого продукта
* инвестируете в проект серьезные средства
* находите высококлассных и очень дорогостоящих профессионалов, умеющих управлять такими проектами
* пытаетесь потом все это продавать

Если Вам это не нужно – будем покупать и внедрять. Покупать готовую систему и внедрять совместно с разработчиком системы или с консалтинговой фирмой-партнером разработчика, с максимальным участием в проекте своих специалистов.

*Какую систему выбрать?*

Если 20% возможностей КИС проработаны так, что удовлетворяют достижению целей и задач автоматизации, то такая система может рассматриваться как кандидат на внедрение.

КИС должна наилучшим образом воплощать выбранные стратегии развития, поэтому нужно:

* сформулировать цели внедрения
* определить желаемый результат
* сформировать перечень важнейших управленческих технологий (бизнес-процессов) – техническое задание на выбор КИС
* ознакомиться с системами и сравнивать – насколько реализованные в каждой из рассматриваемых КИС функций соответствуют описанным в задании

*Внедрить КИС собственными силами?*

|  |  |  |
| --- | --- | --- |
| Локальная система | → | Да  |
|  |  |  |
| Финансово-управленческие системы | → | 50/50 (при наличии службы АСУ хорошо подготовленными специалистами) |
|  |  |  |
| Средняя или крупная интегрированная система | → | Мероприятие рискованное |
|  |  |  |
| КИС | → | Поставляют свои системы только в том случае, если внедрением будут заниматься они сами, или сертифицированные партнеры |

*Зачем нужны консультанты?*

Проект внедрения КИС в коммерческой организации – это проект постановки управленческих технологий с применением средств автоматизации.

К участию могут привлекаться консультанты:

* по управлению
	+ проведут анализ организационной структуры компании и бизнес-процессов, протекающих в компании
	+ помогут руководству в выработке стратегии развития
	+ рекомендуют оптимальные способы разделения обязанностей между отделами и работниками
	+ настроят систему принятия решений и т.д.
* финансовые
	+ помогут поставить на предприятии систему финансового контроллинга:
		- разработают учетную политику
		- систему бюджетов и планов
		- средства контроля деятельности компании и подразделений
		- критерии оценки результатов деятельности
* инвестиционные
	+ «дороговизна» консультантов дешевле, чем использование собственных отделов АСУ
	+ Правило: поставщик КИС и инвестиционный консультант должны быть разными организациями, не зависящими друг от друга
	+ Потребность в обосновании инвестиционных затрат может быть как у владельцев и руководства компании для принятия взвешенного решения о финансировании, так и у внешних инвесторов, если финансирование проекта осуществляется из внешних источников
* IT-консультанты (консультанты по информационным технологиям)
	+ Обследование организации-клиента (желательно – совместно с консультантами по управлению)
	+ Разработка проекта автоматизации
	+ Обучение персонала клиента
	+ Настройка КИС
	+ Координация процесса внедрения
	+ Поддержка и сопровождение КИС на стадии эксплуатации

*С чего начать? Не стоит изобретать велосипед!*

1. Осознайте потребность в автоматизации (концептуальный этап)
	1. Проведите серию совещаний с руководителями подразделений и ключевыми специалистами по возникшим проблемам
	2. Возможно, что проблема кроется совсем не в отсутствии автоматизации
2. Сформулируйте цель внедрения и разбейте ее на конкретные задачи
	1. Цель:
		1. упорядочение материальных и финансовых потоков для наилучшего удовлетворения требований клиентов, снижения потребности в оборотных средствах и максимизации прибыли компании
	2. Задачи – это конкретные блоки проблем, которые необходимо решить, например:
		1. Создать систему бюджетного планирования и контроля расходования средств, основанную на реальных данных
		2. С использованием АСУ реализовать взаимосвязанное планирование продаж, производственной программы, плана по снабжению, плана доходов и расходов
3. Сформируйте рабочую группу по выбору системы
	1. Включите в ее состав руководителей подразделений и ключевых специалистов (нач. службы АСУ и подразделений, через которые проходят основные бизнес-процессы и финансовые потоки)
	2. Члены группы встречаются с поставщиками КИС, независимыми консультантами, посещают выставки, проводят рабочие совещания, на которых обсуждают плюсы и минусы различных вариантов
	3. Создание группы скажется на процессе внедрения: руководители основных подразделений причастны к выбору системы, при внедрении не будут воспринимать КИС как чужое, насажденное извне
4. Выберите консалтинговую компанию или осуществите обследование самостоятельно
	1. Комплексное обследование является не роскошью, а необходимостью
	2. Профессиональный консультант в состоянии провести обследование и подготовить техническое задание независимо от того, какая конкретно КИС будет развернута на предприятии (для проведения данной работы используются определенные стандартные методики, технологии и программные средства)
	3. Составленное на профессиональном языке ТЗ будет понятно для поставщика КИС
5. Выберите КИС и заключите договор на внедрение системы, основываясь на техническом задании и выводах рабочей группы

Когда клиент изначально оказывает доверие поставщику КИС, возможно объединение этапов 4-5. при этом обследование производится специалистами поставщика КИС (сокращает общий срок автоматизации, но повышает риск выбрать не самое лучшее решение).

Личное участие руководителя действительно требуется!

КИС затрагивает интересы множества людей, возникает конфликт интересов – сопротивление неизбежно. Необходимы воля и власть.

*Зачем нужно обследование?*

* Компании необходимо произвести частичную реорганизацию структуры и коррекцию бизнес-технологий
* Отсутствие формализованной системы управления снижает шансы на успешное внедрение КИС до нуля. Нельзя автоматизировать хаос – в результате получится автоматизированный хаос.
* На основе заключения, полученного в результате обследования, строится вся дальнейшая схема построения КИС
* Автоматизацию по принципу «как есть» проводить не следует, так как в результате обследования обычно обнаруживается масса нестыковок, бессмысленных работ, лишних затрат, противоречий в организационной структуре, устранение которых позволило бы уменьшить издержки и существенно сократить время исполнения различных бизнес-процессов

*Реинжиниринг бизнес-процессов*

М. Хаммер: РБП – это фундаментальное перепроектирование бизнес-процессов компаний для достижения коренных улучшений в основных актуальных показателях их деятельности: стоимость, качество, услуги и темпы.

Одной из основных особенностей BPR (РБП) является ориентация не на функции, а на процессы. Хаммер рассматривает РБП как революцию в бизнесе, которая знаменует отход от базовых принципов построения предприятий и превращает конструирование бизнеса в инженерную деятельность.

Многие рассматривают РБП как некое дополнительное мероприятие, приуроченное к внедрению КИС.

Реинжиниринг и внедрение – принципиально разные понятия.

Суть РБП – в построении системы рационального управления предприятием, отправной точкой которой является не программное обеспечение, а взаимодействие человеческих и материальных ресурсов.

Внедряемая КИС представляет собой всего лишь реализацию системы управления предпряитием.

Применение РБП:

1. РБП – не единственный метод осуществления улучшений в бизнесе. Существуют эффективные и менее радикальные методологии, такие как «всеобщее качество» - TQM, или метод «непрерывных улучшений»
2. прежде чем применять РБП, можно привлекать консультантов, почитать книгу Робсона и Уллаха «Практическое руководство по реинжинирингу бизнес-процессов»
3. когда решение о применении метода созрело – начните локально. Если в результате применения РБП выйдет не то, что хотелось, то последствия не будут слишком тяжелыми
4. не стоит проводить реорганизацию всего без веских оснований. Реорганизация может быть проведена в ряде локальных точек, где она объективно необходима, что не повлечет за собой ощутимый спад активности текущей коммерческой деятельности

*Потребуется ли обновление парка вычислительной техники?*

Большинство КИС основаны на так называемой технологии «клиент-сервер». КИС предъявляет существенные требования:

* upgrade или приобретение более мощного сервера
* наведение порядка в сетевой инфраструктуре
* частичное обновление парка ПК пользователей

Разработчики КИС указывают рамочные требования к техническим характеристикам серверов и рабочих станций.

Последовательность внедрения:

1. Создайте команду внедрения. Включите в ее состав руководителей тех подразделений, через которые проходят ключевые бизнес-процессы компании. Не забудьте привлечь наиболее важных и компетентных специалистов.
2. Предпримите меры для преодоления сопротивления сотрудников внедрению КИС. Привлеките кого-то из наиболее ярых противников внедрения к работе во внедренческой команде: этим Вы свяжете ему руки. Разработайте систему мер поощрения и наказания.
3. Создайте у всех стойкое ощущение неизбежности внедрения. Для этого утвердите план-график внедрения, проведите собрание руководителей подразделений, на котором объявите о запуске проекта и сроках его осуществления.
4. Наделите руководителя проекта необходимыми властными полномочиями. Для того, чтобы он смог эффективно преодолевать сопротивление проекту.
5. Организуйте эффективное взаимодействие команды внедрения и представителей поставщика (консультантов). А также тотальное документирование всех проектных решений и результатов: когда консультанты уйдут, это поможет службе АСУ обслуживать и развивать КИС максимально автономно.
6. Попробуйте сначала реализовать пилотный проект. Вы не почувствуете всю мощь системы, но оцените степень компетентности и деловой порядочности поставщика КИС и консультантов.
7. Не обязательно автоматизировать все сразу. При разработке проекта внедрения КИС определите очередность ввода подсистем, график автоматизации подразделений. В первую очередь поставьте ключевые подсистемы, подразделения, компании: КИС начнет приносить отдачу раньше и быстрее окупится.
8. Регулярно контролируйте ход проекта. Вникайте в его ключевые моменты. Анализируйте причины отклонений от графика работ и применяйте управляющие воздействия.
9. Не допускайте внесения существенных дополнений в проект. Только в случае обнаружения грубых ошибок (рискуете погрязнуть в проекте навсегда и исчерпать отведенный лимит финансирования).
10. Не срывать график финансирования. Это приведет к рассогласованию проекта и удлинению сроков внедрения.

|  |  |
| --- | --- |
| Факторы успешного внедрения КИС | % |
| Участие руководства во внедрении | 20 |
| Наличие и соблюдение плана внедрения | 19 |
| Наличие у менеджеров четких целей и требований к проекту | 16 |
| Участие во внедрении специалистов компании-клиента | 16 |
| Качество КИС и команды поставщика решения | 11 |
| Проведение реинжиниринга бизнес-процессов до внедрения | 8 |
| Наличие у предприятия выработанной стратегии | 8 |
| Получение быстрой и ощутимой отдачи | 2 |
|  |  |
| Основные сложности при внедрении КИС | % |
| Невнимание руководства компании к проекту | 40 |
| Отсутствие четко сформулированных целей проекта | 17 |
| Неформализованность бизнес-0процессов в компании | 14 |
| Неготовность компании к изменениям | 12 |
| Нестабильность законодательства | 6 |
| Коррупция в компаниях | 5 |
| Низкая квалификация кадров в компании | 4 |
| Недостаточное финансирование проектов | 2 |

*Риски внедрения*

* Моральная неготовность компании ко внедрению.
	+ Если необходимость внедрения не осознана руководством компании и руководителями важнейших подразделений
	+ Основной риск, подстерегающий предприятие на пути к успешному завершению проекта автоматизации
* Нарушение сроков.
	+ Отсутствие реальной поддержки проекта со стороны руководства, непонимание целей сотрудниками, плохая управляемость внутри компании – неисполнение или несвоевременное исполнение проектных задач
	+ неграмотно разработанного проекта или принятия популистских решений типа «Создать к 7 ноября» в угоду чьим-то интересам, а также недофинансированность проекта
* Перерасход бюджета.
	+ После утверждения проектной документации возникают различные дополнительные требования и хотения (это нужно в корне пресекать, все «прибамбасы» следует оставить на будущее)
	+ Неграмотно составленный бюджет(никто не оспаривает необходимость минимизировать проектные расходы, однако во всем нужно знать меру: «канарейка за копейку» не получится)
* Нехватка ресурсов
	+ Утверждая проект, «добрый» директор широким росчерком пера подпишет смету с N-нулями, не позаботившись об источниках средств
	+ Такой проект обречен на провал: ни один поставщик КИС или консультант не станет работать задаром из-за того, что компания не позаботилась о финансировании

*Внедрили… что дальше?*

1. На стадии эксплуатации внедренческий процесс не останавливается – он проходит спокойно и локально, реализуется в большинстве случаев силами своей службы АСУ.
2. Успешно функционирующая КИС формирует в компании совершенно иной климат. Сотрудники компании, убедившись в полезности и эффективности системы, начинают более осмысленно относиться к информации, возрастаю их возможности в области обработки информации, появляются дополнительные требования к системе.

*За что берут ежегодные сборы?*

* Выпустив продукт на рынок, разработчики КИС продолжают его совершенствовать
* Государственные ведомтсва непрерывно меняют законодательство
* Стоимость годовой поддержки обычно составляет от 15 до 30% от стоимости купленных лицензий
* Стоимость первого года поддержки входит в их стоимость, но со второго года придется платить дополнительно
* Годовая поддержка – дело добровольное, но чтобы получить новую версию Вас вежливо попросят за нее заплатить
* Некоторые поставщики предложат оплатить поддержку за неоплаченный период, после чего предоставят обновленную КИС

Удовлетворенности заказчиков ходом и результатами внедрения КИС

Основные особенности внедрения КИС (отчет Boston Consulting Group (BCG):

* соответствие проектов внедрения плановым показателям оценивается для ERP-систем в 60%
* из них «досрочные» внедрения – около 3%
* полностью провалившиеся проекты – в 10%
* 60% респондентов считают, что их усилия по внедрению ERP-систем принесли значительную пользу
* 52% полагают, что они достигли поставленных бизнес-целей
* 37% отмечают ощутимое финансовое воздействие от внедрения КИС

В ходе опроса выявлен и рост неудовлетворенности заказчиков разработчиками КИС:

* 15% считают, что разработчики КИС не фокусируются на целях ведения бизнеса
* 33% полагают, что разработчики КИС поощряют неоправданные расходы
* 12% просто расторгли контракт со своим первым разработчиком КИС

Многие респонденты осознают, что цена внедрения КИС слишком высока. Каждый пятый респондент, внедривший у себя на предприятии ERP или SCM-приложения, считает, что мог сделать это же за меньшую цену (эти же респонденты полагают, что более половины расходов были излишни).

Респонденты считают КИС меньшей стоимость лучшими. Средняя стоимость проектов по внедрению КИС, получивших положительную оценку, составляет $10 млн.

Средняя стоимость проекта с отрицательной оценкой - $90 млн.

Эффективное исполнение проекта по внедрению КИС не всегда удовлетворяет заказчика. У 58% респондентов с положительной оценкой результатов внедрения КИС исполнители проектов завершили их в срок и в рамках бюджета.

Аналогичная картина характерна и для 33% респондентов с отрицательным отношением к результатам внедрения КИС.

Формулирование стратегий и целей являются главным фактором успешного внедрения КИС:

* проекты, основанные на ясном стратегическом видении и стратегических оценках, достигли положительных результатов в 53% случаев (22% - при отсутствии такого стратегического подхода). По мнению опрошенных, ключевым фактором для успеха внедрения является тщательный анализ текущей ситуации.
* Проекты, в которых проводился подробный анализ бизнес-возможностей (с учетом действий конкурента, лучших показателей для ведения бизнеса, а также существующей практики бизнеса), достигли положительных результатов в 56% случаев (и только в 8% случаев, когда такой анализ не проводился).

Респонденты также отмечают необходимость частого пересмотра опций и альтернатив:

* проекты, реализованные после тщательной оценки опций и альтернатив (то есть, простого перехода на более современное ПО, проведения перестройки производственных процессов и использования промежуточных решений) достигли положительных результатов в 43% случаев (и только 9% случаев, когда эти опции во внимание не принимались).
1. Участники мирового рынка КИС предпочитают говорить скорее о своем опыте «продуктивных», а не «успешных» внедрений (например, компания SAP AG).
2. О «продуктивных» внедрениях имеет смысл говорить и в случае частичной реализации КИС на предприятии, т.е. отдельных модулей (что характерно как для российских, так и для западных предприятий).

**Тема 7 Актуальность защиты информации.**

**1. Сущность информационной безопасности**

С точки зрения информационной безопасности (ИБ) информация – данные, представленные в виде, пригодном для хранения, обработки и передачи, и представляющие определенную ценность.

Существуют следующие формы представления информации:

электронная,

печатная,

визуальная,

аудио-форма.

Защита информации (ЗИ) – комплекс мероприятий по обеспечению конфиденциальности, целостности, доступности, учета и неотрекаемости информации.

Конфиденциальность – состояние информации, при котором ознакомиться с ней могут только уполномоченные лица.

Целостность – состояние информации, при котором изменять её могут только уполномоченные лица.

Доступность – возможность получения авторизованного доступа к информации со стороны уполномоченных лиц.

Учёт – фиксация и анализ всех действий уполномоченных лиц, выполняемых ими в рамках, контролируемых системой ИБ.

Неотрекаемость – предполагает, что отправитель информации не может отречься от факта отправления, а получатель – от факта получения.

Уполномоченными лицами считаются владелец информации и пользователи, получившие право работы с информацией от ее владельца.

Информационная система (ИС) – совокупность объектов и субъектов информационного взаимодействия.

Объекты – информационные ресурсы. Субъекты – пользователи или процессы, обрабатывающие информацию.

ИБ – более широкое понятие, чем понятия "защита информации", компьютерная безопасность", "сетевая безопасность", "безопасность данных".

ИБ – комплекс мероприятий по защите информации и обеспечению безопасного функционирования ИС

Информационное пространство – совокупность информационных систем, взаимодействующих между собой, причем одна часть этих систем может иметь интересы, прямо противоположные интересам другой.

Т.о. ИБ предполагает защиту одних ИС от других.

Для любой ИС характерны следующие понятия:

Угроза – возможность реализации несанкционированных действий (НД) в отношении ИС.

Уязвимость – незащищенность или ошибка в объекте, которая может привести к возникновению угрозы

Атака – попытка практической реализации угрозы (успешная или нет).

Ошибка – непреднамеренное незапланированное действие, совершаемое субъектом, которое представляет или может представлять угрозу ИБ.

Авария – неумышленное происшествие с деструктивным воздействием на объект.

Злоумышленник – субъект, преследующий корыстные или деструктивные цели, противоречащие целям системы.

**2. Классификация  конфиденциальной информации**

Говоря о защите какой-либо информации, следует прежде всего вы­яснить, к какой категории она относится. Существует следующая класси­фикация тайн по шести категориям:

государственная тайна,

коммерческая тайна,

банковская тайна,

профессиональная тайна,

служебная тайна,

персональные данные.

Последние пять категорий составляют конфиденциальную информацию.

Слово "конфиденциальный" происходит от латинского confidentia - доверие и в современном русском языке означает "доверительный, не подлежащий огласке, секретный. Слово "секрет" заимствовано из французского secret - "тайна". В знаменитом словаре В. Даля также названы аналогичные значения: "конфиденциальная" - "откровенная, по особой доверенности, неоглашаемая, задушевная"; "тайна" - "кто чего не знает, то для него тайна, все сокрытое, неизвестное, неведомое".

Таким образом, точки зрения этимологии можно сделать вывод о равнозначности понятий конфиденциальная информация, тайна и секрет.

Однако понятие тайны в правовой науке не полностью совпадает с понятием конфиденциальной информации, так как тайна означает ещё и правовой режим информации. В соответствии со ст. 2 ФЗ "Об информации ..." и ст. 2 ФЗ "Об участии в международном информационном обмене", конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. Но не всегда информация с ограниченным доступом является документированной, например сведения, составляющие личную и семейную тайну, не обязательно зафиксированы на материальном носителе.

При анализе видов конфиденциальной информации возникают большие сложности, связанные с противоречивостью и недостатками отечественного законодательства. Согласно п. 2 ст. 10 ФЗ "Об информации ...", документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

Наиболее важными являются сведения, относящиеся к государственной тайне. В Законе "О государственной тайне" дано следующее определение:
"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.

В законодательстве предусматривается наличие различного рода сведений, не содержащих гостайну, которые также охраняются законом. Так, охраняется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, личная и семейная тайна (ст.23 Конституции РФ). Кроме того, сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ст.24).

Подлежащую защите информацию можно сгруппировать по следующим основаниям:

собственники информации;

области (сферы) деятельности, в которых используется информация

лица и организации, на которых возложена защита данной информации.

Ту же информацию, подлежащую защите можно классифицировать по трем признакам:

по принадлежности,

по степени конфиденциальности (степени ограничения доступа),

по содержанию.

По принадлежности владельцами защищаемой информации могут быть:

органы государственной власти и образуемые ими структуры (государственная тайна, служебная тайна, в определенных случаях коммерческая и банковская тайны);

юридические лица (коммерческая, банковская служебная, адвокатская, врачебная, аудиторская тайны и т.п.);

граждане (физические лица) - в отношении личной и семейной тайны, нотариальной, адвокатской, врачебной.

По степени конфиденциальности (степени ограничения доступа) в настоящее время можно классифицировать только информацию, составляющую государственную тайну. Согласно ст.8 Закона РФ "О государственной тайне", устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений:

"особой важности",

"совершенно секретно",

"секретно".

Для остальных видов тайн данное основание классификации пока не разработано, при этом согласно ст. 8 Закона РФ "О государственной тайне", использование названных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

По содержанию защищаемая информация может быть разделена на политическую, экономическую, военную, научную, технологическую, личную, коммерческую и т.п.

Конфиденциальная информация бывает двух видов: подлежащая обязательной защите и не подлежащая. Обязательность защиты определяется собственником информации, за исключением случаев, предусмотренных законодательством. Так, в Законе говорится, что конфиденциальная информация государственных органов подлежит обязательной защите.

Указом Президента вводится шесть категорий конфиденциальной информации:

Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

Сведения, составляющие тайну следствия и судопроизводства.

Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

**Служебная информация**

В Гражданском кодексе РФ дается следующее определение служебной информации: "Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности".

В "Положении о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти" (утверждено Постановлением Правительства Российской Федерации № 1233 от 3 ноября 1994г.) вводится понятие служебной информации ограниченного распространения: "несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью".
         В государственных структурах еще может быть информация, имеющая политическую или иную ценность. Поскольку к служебной тайне она не относится, ей также необходимо присваивать гриф "для служебного пользования", применяемый в органах исполнительной власти.

**3**. **Современная концепция ИБ**

Концепция ИБ является методологической основой для формирования и проведения в организации или на предприятии единой политики в области обеспечения ИБ.

Современная КИБ включает в себя следующие разделы:

цели и задачи обеспечения ИБ,

категории объектов защиты,

перечень угроз безопасности,

неформальная модель нарушителя,

принципы построения и направления работ по созданию и поддержанию СИБ,

средства обеспечения ИБ,

механизм функционирования СИБ.

**Цели и задачи обеспечения ИБ**

Основная цель обеспечения ИБ – защита субъектов информационных отношений (ИО) отвозможного нанесения им материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования ИС или НСД к циркулирующей в ней информации и ее незаконного использования.

Субъекты ИО заинтересованы в обеспечении:

конфиденциальности информации,

целостности информации,

своевременного доступа к информации,

защиты от дезинформации,

разграничения ответственности за нарушения законных прав (интересов) других субъектов ИО и установленных правил обращения с информацией,

возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации,

защиты части информации от незаконного ее тиражирования.

Для достижения основной цели защиты СИБ должна обеспечивать эффективное решение следующих задач:

защита от вмешательства в процесс функционирования ИС посторонних лиц,

обеспечение аутентификации субъектов, участвующих в информационном обмене,

управление доступом уполномоченных лиц к аппаратным, программным и информационным ресурсам ИС,

регистрация действий пользователей при использовании защищаемых ресурсов,

контроль и поддержание целостности среды исполнения программ,

защита от несанкционированной модификации и контроль целостности используемых в ИС программных средств,

защита ИС от внедрения несанкционированных программ,

защита конфиденциальной информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи,

своевременное выявление новых источников угроз безопасности информации,

создание условий для минимизации и локализации наносимого ущерба и ликвидация последствий нарушения ИБ.

**Категории объектов защиты**

Основными объектами защиты являются:

информационные ресурсы с ограниченным доступом, представленные в виде документов и массивов информации, независимо от формы и вида их представления;

процессы обработки, хранения и передачи информации,

информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, системы и средства защиты информации, объекты и помещения, в которых размещены компоненты ИС,

персонал разработчиков и пользователей ИС и ее обслуживающий персонал.

**ТЕМА 8 Источники, риски и формы атак на компьютерную информацию.**

* 1. **Основные объекты защиты информации**

Под угрозой безопасности информации подразумевают действия или события, которые могут привести к несанкционированному использованию, искажению или к разрушению информационных ресурсов системы, аппаратных и программных средств.

**Основными объектами информации являются:**

Информационные ресурсы, содержащие сведения, связанные с конфиденциальной информацией и государственной тайной.

Информационные системы (сети и системы, средства вычислительной техники), программные средства (операционные системы, системы управления базами данных, прикладное программное обеспечение), технические средства приёма, автоматизированные системы управления, системы связи и передачи данных, передачи и обработки информации ограниченного доступа (звукозапись, звукоусиление, звуковоспроизведение, переговорные и телевизионные устройства, средства тиражирование и изготовления документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), т.е. все системы и средства, обрабатывающие секретную (конфиденциальную), информацию относящуюся к государственной тайне. Все эти перечисленные средства и системы называют техническими средствами приёма, обработки и хранения информации (ТСПИ).

Технические средства и системы, не входящие в состав ТСПИ, но расположенные в помещениях обработки конфиденциальной информации. Данное оборудование называется вспомогательными техническими средствами и системами (ВТСС). Оно состоит из следующих компонентов: системы пожарной и охранной сигнализации, технические средства телефонной, громкоговорящей связи, радиотрансляции, часофикации, контрольно-измерительная аппаратура, средства и системы передачи данных в системе радиосвязи, электробытовые приборы, а также сами помещения, предназначенные для обработки данной информации имеющей ограниченное распространение.

ТСПИ можно рассматривать как систему, включающую в себя стационарное оборудование, соединительные линии, периферийные устройства, системы электропитания, распределительные и коммуникационные устройства и системы заземления.

Все технические средства, предназначенные для обработки секретной информации, включая помещения, в которых они расположены, представляют собой объект ТСПИ.

**1.2 Виды угроз**

Исследования случаев воздействия на информацию и несанкционированного доступа к ней показывают, что их можно разделить на случайные и преднамеренные. Преднамеренные угрозы часто могут быть приведены в исполнение, путем их систематического применения через долговременные, массированные атаки, несанкционированные запросы или вирусы.

Если задача по преднамеренным угрозам выполняется, то это может привести к следующим последствиям:

* разрушению информации;
* модификации - изменению информации на ложную, похожую по своему содержанию и форме, но имеющею другой смысл;
* ознакомлением с ней третьих лиц.

Итог данных событий может быть различным: от невинных недоразумений до огромных убытков или ослабления безопасности. Основной целью создания систем безопасности и является предупреждение данных последствий.

**1.2.1 Случайные угрозы**

Многочисленные исследования проектирования, испытаний и эксплуатации автоматизированных систем показывают, чтолюбая информация в процессе ввода, обработки, хранения, вывода и передачи подвергается разнообразным случайным воздействиям. В результате данных воздействий на аппаратном уровне в цифровых кодах происходят физические изменения уровней сигналов, несущих информацию.

А именно в одном, двух, трех или других разрядах изменения 0 на 1 или 1 на 0, или то и другое вместе, но в разных разрядах, следствием чего в итоге является незначительное изменение значения кода. Если средства функционального контроля, применяемые для этой цели способны обнаружить данные изменения (например, контроль по модулю 2 легко обнаруживает однократную ошибку), производится браковка данного кода, а устройство, модуль, микросхема или блок, участвующие в обработке, объявляются неисправными. Если данный функциональный контроль отсутствует, либо не способен обнаружить неисправность на данном этапе обработки, процесс обработки происходит по ложному пути, т. е. происходит случайная модификация информации. В результате данной ошибки, при дальнейшей обработке информации возможна передача ложной информации адресату, пересылка информации по ложному адресу, либо стирание или запись другой информации в ОЗУ или ДЗУ, а именно возникновение нежелательных событий: разрушение (утрата), модификация и утечка информации.

Основными причинами случайных воздействий на автоматизированные системы при их эксплуатации могут быть:

* сбои и отказы аппаратуры;
* помехи на линиях связи от воздействия внешней среды;
* ошибки человека как звена системы;
* системотехнические и схемные ошибки разработчиков;
* алгоритмические, структурные и программные ошибки;
* аварийные ситуации.
* к показала практика при выборе и проектировании системы, слабой в отношении надежности функционирования аппаратуры, частота отказов и сбоев аппаратуры увеличивается.

**1.2.2 Преднамеренные угрозы**

Преднамеренные угрозы обычно связаны с действиями, какого либо человека, причинами которых могут выступать определенное недовольство своей жизненной ситуацией, а именно материальный интерес или простое развлечение с самоутверждением своих способностей, как у хакеров.

Преднамеренные угрозы можно разделить на пассивные и активные.

Пассивные угрозы - предназначены в основном на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на нормальную работу самой системы. К пассивным угрозам можно отнести несанкционированный доступ к базам данных, прослушивание каналов связи.

Активные угрозы - имеют цель нарушения нормальной работы системы, путем целенаправленного воздействия на ее компоненты. К активным угрозам можно отнести, например, вывод из строя операционной системы компьютера, разрушение ПО компьютеров, нарушение работы линий связи и т.д.

Преднамеренные угрозы так же могут быть**:**

* внутренние угрозы - возникающие внутри самой управляемой организации;
* внешние угрозы - возникающие из вне, как правило, обусловленные действиями конкурентов.

К основным угрозам безопасности информации от разрушения, модификации и ознакомления с ней третьих лиц относятся:

* утечка конфиденциальной информации;
* компрометация информации;
* ошибочное использование информационных ресурсов;
* нарушение информационного обслуживания;
* несанкционированный обмен информацией между абонентами;
* несанкционированное использование информационных ресурсов;
* незаконное использование привилегий.

Утечка конфиденциальной информации -- это бесконтрольный выход конфиденциальной информации за пределы контролируемой зоны или круга лиц, которым она была доверена по службе или стала известна в процессе работы.

При применении к какой либо организации или структуре любого вида шпионажа возможен бесконтрольный уход конфиденциальной информации по техническим каналам связи. Рассмотрим их более подробно.

**1.2.3 Технические каналы утечки информации**

Наибольшую возможность образования каналов утечки информации представляют ТСПИ и ВТСС, имеющие непосредственный выход за пределы контролируемой зоны (КЗ).

Контролируемая зона - это территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа. Контролируемая зона может ограничиваться периметром охраняемой территории, либо большим размером, чем охраняемая территория, но при этом она должна обеспечивать постоянный контроль за неохраняемой частью территории.

Кроме соединительных линий ТСПИ и ВТСС за пределы данной зоны могут выходить проходящие через помещения посторонние проводники, непредназначенные для ТСПИ и ВТСС (рис. 1.1).

Зона с возможностью захвата разведывательным оборудованием побочных электромагнитных излучений, содержащих секретную информацию, называется опасной зоной. Окружающие пространство вокруг ТСПИ, в котором на случайных антеннах наводится информационный сигнал выше допустимого уровня, называется опасной зоной.

Случайными антеннами являются цепи ВТСС или посторонние проводники, воспринимающие побочные электромагнитные излучения от средств ТСПИ. Случайные антенны бывают:

* сосредоточенными (технические средства с сосредоточенными параметрами, такие как телефонный аппарат, радиотрансляционной громкоговоритель сети);
* распределёнными (их образуют проводники с распределёнными параметрами, такие как соединительные провода, кабели, металлические трубы).

Информационные сигналы могут быть электрическими, акустическими электромагнитными и т.д. Они по своей природе в большинстве случаев имеют колебательный характер, а информационными параметрами являются амплитуда, длительность, фаза и частота.

Технический канал утечки информации (ТКУИ) можно рассмотреть как составляющую объекта разведки, технического средства разведки (TCP) и физической среды, непосредственно в которой распространяется данный информационный сигнал. В сути, под ТКУИ подразумевают способ получения с помощью TCP любой разведывательной информации об объекте.

В зависимости от природы возникновения сигналы распространяются в некоторых физических средах. Так средой распространения могут являться твердые, газовые (воздушные) и жидкостные (водные) среды. К данным средам относят воздушное пространство, соединительные линии и токопроводящие элементы, конструкции зданий, грунт и другие.

Противодействие экономическому и промышленному шпионажу является постоянным и адекватным процессом развития методов, средств и способов защиты информации от новых типов угроз.

Классификация каналов утечки информации.

Технические каналы утечки информации обрабатываемой ТСПИ

I. Электромагнитные:

* электромагнитные излучения элементов ТСПИ;
* электромагнитные излучения на частотах роты ВЧ-генераторов ТСПИ;
* излучения на частотах самовозбуждения усилителей низкой частоты.

II. Электрические:

* наводки электромагнитных излучений элементов ТСПИ на посторонние проводники;
* просачивание информационных сигналов в линии электропитания;
* просачивание информационных сигналов в цепи заземления;
* съем информации с использованием закладных устройств.

III. Параметрические:

- перехват информации путем «высокочастотного облучения» ТСПИ;

IV. Вибрационные:

- соответствие между распечатываемым символом и его акустическим образом.

Технические каналы утечки информации при передаче ее по каналам связи

I. Электромагнитные:

- электромагнитные излучения передатчиков связи, модулированные информационным сигналом (прослушивание радиотелефонов, сотовых телефонов, радиорелейных линий связи).

II. Электрические:

- подключение к линиям связи.

III. Индукционный канал:

- эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов.

IV. Паразитные связи:

- паразитные емкостные, индуктивные и резистивные связи и наводки близко расположенных друг от друга линий передачи информации.

Технические каналы утечки речевой информации

I. Акустические каналы:

- среда распространения - воздух.

II. Виброакустические каналы:

- среда распространения - ограждающие строительные конструкции.

III. Параметрические каналы:

- результат воздействия акустического поля на элементы схем, что приводит к модуляции высокочастотного сигнала в информационный.

IV. Акустоэлектрические каналы:

- преобразование акустических сигналов в электрические.

V. Оптико-электронный канал (лазерный):

- облучение лазерным лучом вибрирующих поверхностей.

Технические каналы утечки видовой информации

I. Наблюдение за объектами:

- для наблюдения днем применяются оптические приборы и телевизионные камеры;

- для наблюдения ночью - приборы ночного видения, телевизионные камеры, тепловизоры.

II. Съемка объектов:

- для съемки объектов используются телевизионные и фотографические средства. Для съемки объектов днем с близкого расстояния применяются портативные камуфлированные фотоаппараты и телекамеры, совмещенные с устройствами видеозаписи

III. Съемка документов:

- Съемка документов осуществляется с использованием портативных фотоаппаратов.

Перечисленные пути несанкционированного доступа по техническим каналам требуют достаточно профессиональных технических знаний и соответствующих программных или аппаратных разработок со стороны взломщика.

Однако злоумышленники не пренебрегают и другими способами добычи нужной информации, такими как: инициативное сотрудничество; склонение к сотрудничеству со стороны взломщика; хищение носителей информации и документальных отходов; подслушивание; выпытывание и другие.

**ТЕМА 9 МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ**

**2.1 Методы инженерно-технической защиты информации**

Теория инженерно-технической защиты информации описывает основные принципы, средства и методы обеспечения информационной безопасности объектов. Она включает в себя следующие вопросы**:**

- систему защиты информации;

- оценку угроз;

- принцип построения системы защиты информации.

Инженерно-техническая защита состоит из таких компонентов, как специальные органы, технические средства и мероприятия по их использованию для защиты конфиденциальной информации.

Постоянная и эффективная техническая защита информационных ресурсов является обязательной составляющей комплексной системы обеспечения информационной безопасности и способствует оптимизации денежных расходов на организацию защиты информации. Техническая защита информации предполагает целый комплекс мероприятий по защите информации от несанкционированного доступа по различным видам каналов, а также исключения специальных воздействий на нее, таких как, уничтожение, искажение или блокирование доступа.

Основными целями и задачами технической защиты являются:

- защита носителей информации от полного уничтожения в результате различных природных и техногенных воздействий;

- предотвращение проникновения злоумышленника к источникам информации с целью уничтожения, хищения или изменения;

- предотвращение утечки информации по различным техническим каналам.

При проектировании систем технической защиты необходимо выполнять следующие принципы:

- непрерывность защиты информации в пространстве и во времени, постоянная готовность и высокая степень эффективности по ликвидации угроз информационной безопасности;

- многозональность и многорубежность защиты, задающее размещение информации различной ценности во вложенных зонах с контролируемым уровнем безопасности;

- избирательность в выборе первоочередности защиты наиболее важной информации;

- интеграция (взаимодействие) различных систем защиты информации с целью повышения эффективности многокомпонентной системы безопасности;

- создание централизованной службы безопасности в интегрированных системах.

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

- инженерные средства, представляющие собой различные сооружения и устройства, предотвращающие физическое проникновение злоумышленников на защищаемые объекты;

- аппаратные средства, представляющие собой измерительные приборы и устройства, программно-аппаратные комплексы, предназначенные для выявления каналов утечки информации, оценки их характеристик по защите информации;

- программные комплексы и средства системы защиты информации в информационных системах различного назначения и в основных средствах обработки данных;

- криптографические средства защиты компьютерной информации, передаваемой по открытым каналам передачи данных и сетям связи.

В концепции инженерно-технической защиты информации кроме целей и задач системы безопасности, определяются принципы ее организации и функционирования; правовые основы; виды угроз и ресурсы, подлежащие защите, а также основные направления разработки системы безопасности.

К основным целям защиты информации относятся: предотвращение утечки, утраты, хищения, искажения, подделки информации и применение других несанкционированных негативных воздействий.

Разработка и создание новой системы защиты, а также оценка эффективности существующей системы безопасности объекта начинается с анализа наиболее возможных угроз и оценки их реального появления. Для получения данных такого рода, необходимо произвести обследование объекта на наличие уязвимостей в защите, а так же учесть особенности расположения, инженерных конструкций, коммуникаций и тому подобного. Следующим этапом выполняется выбор соответствующих методов и средств адекватной защиты объекта.

При рассмотрении вероятных угроз объекту нельзя забывать про угрозу безопасности здоровья персонала; угрозу целости и сохранности оборудования и материальных ценностей; безопасность информации и сохранность государственной или коммерческой тайны.

При проектировании защиты в комплексную систему должно вписываться все-то разнообразие возможных информационных угроз, так как она должна обеспечивать надежное перекрытие всех опасных каналов утечки информации.

Эффективность всей системы защиты от утечки информации по техническим каналам оценивается по разнообразным критериям, которые определяются физической природой информационного сигнала, но чаще всего по соотношению «сигнал/шум».

Все способы защиты согласно руководящей документации делятся на две группы, такие как, скрытие и дезинформация.

К группе скрытие относятся:

- пассивное скрытие - заключается в исключении или значительном затруднении обнаружения объектов;

- активное скрытие - в создании техническим средствам разведки маскирующих шумовых помех различной физической природы и ложной обстановки по физическим полям;

- специальная защита - заключается в скремблирование телефонных переговоров, кодирование цифровой информации криптографическими методами, программные методы модификации информации.

К группе дезинформация относятся:

- техническая дезинформация;

- имитация;

- легендирование.

К принципам инженерно-технической защиты информации относятся:

- скрытность защиты информации;

- надежность защиты информации;

- непрерывность защиты;

- рациональность защиты;

- комплексное применение различных способов и средств защиты;

- многообразие способов защиты;

- экономичность защиты.

**2.2 Виды защиты информации от утечки по техническим каналам**

Для защиты информации от утечки и снижению паразитных связей по техническим каналам используется ряд средств, представляющих собой комплекс поработанных мероприятий. Рассмотрим несколько основных:

**2.2.1 Экранирование электромагнитных волн**

Экранирование электромагнитных волн является одним из самых действенных средств защиты объекта от утечки информации по техническим каналам и основой экологической безопасности.

Но для более эффективной защиты мало просто применить экранирование и развязывающие фильтры на каналы связи, но также в первую очередь необходимо устранять или ослаблять до допустимых значений паразитные связи путем следующих мероприятий:

- размещение вероятных источников и приемников наводок на максимально допустимом расстоянии друг от друга;

- сведение к минимуму общих сопротивлений;

- уменьшение сечения габаритов токонесущих элементов, обеспечивающих минимум паразитной связи (для получения минимальной взаимоиндуктивности катушек индуктивности их оси должны быть взаимно перпендикулярны);

- изъятие посторонних проводов, проходящих через несколько узлов или блоков, которые могут связать элементы, расположенные на удаленном растоянии друг от друга;

- при невозможности исключения посторонних проводов, создающих паразитную связь, необходимо позаботиться о том, чтобы при емкостной паразитной связи сопротивление постороннего провода относительно корпуса было минимальным, при индуктивной паразитной связи необходимо увеличивать внутреннее сопротивление посторонней линии связи.

Экранирование - это локализация электромагнитной энергии в пределах определенного пространства путем преграждения ее распространения.

Развязывающий фильтр - это устройство, ограничивающее распространение помехи по проводам, являющимся общими для источника и приемника наводки.

В настоящее время все актуальней становится проблема формирования электромагнитной обстановки, обеспечивающей нормальное функционирование электронных устройств и экологическую безопасность.

Для создания благоприятной электромагнитной обстановки и обеспечения требований по электромагнитной безопасности объекта, которая включает в себя и предотвращение несанкционированного доступа к информации с использованием специальных технических средств, производится экранирование электромагнитных волн.

Применение качественных экранов позволяет решить многие задачи, в которые входит защита информации в помещениях и технических каналах, электромагнитную совместимость оборудования и приборов при совместном использовании, защиту персонала от повышенного уровня электромагнитных полей и обеспечение безопасной экологической обстановки вокруг работающих электроустановок и СВЧ-устройств.

**2.2.2 Безопасность оптоволоконных кабельных систем**

**Важными характеристиками волоконно-оптических систем передачи информации (ВОСПИ) являются:**

- слабое затухание сигнала и его маленькая зависимость от длины волны передаваемого информационного оптического сигнала, распределения мод и температуры кабеля;

- очень слабое искажение сигнала и его незначительная зависимость oт спектральной ширины, распределения мод, амплитуды и длины волны передаваемого информационного оптического сигнала, температуры окружающей среды и длины световода;

- малые потери на излучение и их незначительная зависимость от радиуса изгиба и температуры волоконного световода;

- простота укладки, сращивания и ввода излучения в световод;

- более приемлемые физические параметры - вес, размер, объем;

- высокая устойчивость к внешним воздействиям - теплостойкость, влагостойкость, стойкость к химической коррозии и к механическим нагрузкам.

Несмотря на перечисленные выше преимущества, у ВОСПИ также присутствуют недостатки, главным из которых является возможность утечки информации за счет побочного электромагнитного излучения и наводок (ПЭМИН) как в оптическом, так и в радиочастотном диапазонах.

Оптоволокно - представляет собой обычное стекло, передающее электромагнитную энергию в инфракрасном диапазоне волн. Излучение наружу практически не просачивается. Эффективный захват информации возможен только путем непосредственного физического подключения к оптоволоконной линии. Но если ВОСПИ рассматривать как систему в целом, содержащую рабочие станции, интерфейсные карты, серверы, концентраторы и другие сетевые активные устройства, которые сами непосредственно являются источником излучений, то проблема утечки информации становятся актуальной. Исходя их этого принимая решения об использовании оптоволоконных кабельных систем (ОКС), нельзя не учитывать этот фактор.

Основным элементом оптоволоконного кабеля является внутренний сердечник из стекла или пластика (рис. 2.1, позиция 1). Диаметр и прозрачность стекловолокна напрямую определяют количество передаваемого им света.

Широко распространены следующие типы оптоволоконного кабеля:

- с сердечником 8,3 мк и оболочкой 125 мк;

- с сердечником 62,5 мк и оболочкой 125 мк;

- с сердечником 50 мк и оболочкой 125 мк;

- с сердечником 100 мк и оболочкой 145 мк.

Оптоволоконные кабели толщиной в 8,3 микрона очень сложно соединить точно. В силу этого возможны монтажные ошибки, в том числе и трудно выявляемые при тестировании кабельной линии. Данные дефекты можно устранить установкой дополнительных оптоволоконных повторителей (концентраторов), но это обуславливается увеличением уровня электромагнитных излучений кабельной системы в целом. Для предотвращения данной проблемы стали изготавливать заказные кабельные комплекты, то есть кабели с уже смонтированными и проверенными в заводских условиях коннекторами, исключающими процедуры монтажа и тестирования линии в полевых условиях.

Для оптоволоконного кабеля характерны следующие особенности:

- наличие центрального силового элемента;

- размещение в полимерной трубке-модуле;

- количество оптических волокон в одном модуле - от 1 до 12;

- покрытие всех этих элементов и модулей промежуточной полимерной оболочкой;

- заполнение пространства между модулями упрочняющими элементами (корделями из стеклонитей или нитей из кевлара и гидрофобным гелем);

- внешняя защита оболочки из полиэтилена или металла (также возможно наличие двух защитных оболочек - металлической и полиэтиленовой).

Наряду с перечисленными общими особенностями оптоволоконные кабели различных моделей могут иметь дополнительные скрепляющие ленты, антикоррозийные и водозащитные обмотки, гофрированные металлические оболочки и т.д.

Как уже писалось, наиболее эффективным способом перехвата информации с оптоволоконных кабельных систем является непосредственное подключение к ним. Появилась информация о создании специальных дистанционно управляемых роботов, которые способны самостоятельно передвигаться по кабельным канализациям и производить подключение к оптоволоконному кабелю для последующей передачи данных, проходящих в ОКС.

Для предотвращения подключения злоумышленников, имеющим специальную технику, было предложено использовать внутренние силовые металлические конструкции оптоволоконных кабелей в качестве сигнальных проводов. Что сделало невозможным подключением к оптоволокну без нарушения целостности силовых конструкций. При нарушение целостности металлических конструкций происходит срабатывание сигнализации в центре контроля за ОКС. Дополнительного оборудования для контроля над охранной системой практически не требуется.

**2.2.3 Особенности слаботочных линий и сетей как каналов утечки информации**

При рассмотрении задачи обеспечения безопасности помещения нельзя забывать про то что, злоумышленник может использовать телефонные и электросиловые линии, проходящие в здании.

Электросиловые линии в помещениях используются для подслушивания разговоров, через которые проходит линия. Обычно, силовая линия используется в качестве источника питания для подслушивающих устройств, передающих информацию из помещения по радиоканалу. Также линия может использоваться и в качестве проводного канала. Достоинством такого канала передачи выступает большая, чем у радиоканала, скрытность, а недостатком - что приемник информации необходимо подключать к этой же линии и не дальше первой трансформаторной подстанции.

В процессе использования электросиловой линии в качестве источника питания подслушивающее устройство может быть подключено как последовательно, так и параллельно линии. Параллельное подключение является более предпочтительным, из-за того что, устройство для питания использует напряжение линии и может работать в любое время.

Для увеличения скрытности устройства при параллельном подключении могут использоватся так называемые «сторожевые устройства», производящие отключение от сетевых проводов на заданное время при кратковременном пропадании сетевого напряжения в линии. Последовательное подключение является менее удобно для работы подслушивающего устройства, так как в данном случае для питания используется ток линии, а он появляется в линии только при подключении нагрузки.

**Телефонные линии используются:**

- для прослушивания телефонных разговоров (линия используется, как источник информационного сигнала, а также может при этом выполнять функции источника питания);

- для прослушивания разговоров в помещениях, вблизи которых проходит телефонная линия (телефонная линия используется как скрытный канал передачи информации в любое место, где есть телефон, и как источник питания);

- в качестве бесплатного канала телефонной связи (междугородные переговоры за чужой счет) и для проникновения в банковскую компьютерную сеть для присвоения денег (в случае, когда используется телефонная линия для пересылки финансовых документов).

Для подслушивания телефонных разговоров специализированное радиоэлектронное устройство должно быть подключено в любом доступном для злоумышленников месте (в помещениях, в которых проходит линия; в телефонном аппарате; в распределительных коробках и шкафах здания; в узловых распределительных шкафах городской телефонной сети; на АТС) и подключаться параллельно линии (гальванически) или последовательно (гальванически или индуктивно).

При подслушивании разговоров в помещении специальное радиоэлектронное устройство должно быть подключено только в помещении, в котором проходят разговоры, и включаться только параллельно линии (гальванически). Работа данного устройства возможна только когда не используются телефонная линия.

В качестве канала телефонной связи, а также для проникновения в банковскую систему, радиоэлектронное устройство может быть подсоединено в любом доступном для злоумышленников месте, при помощи параллельного подключения (гальванически) и работать только в то время, когда телефонной линией не пользуются.

Для предотвращения прослушивания переговоров существует ряд устройств - анализаторов позволяющих: обнаружить блоки питания специальных радиоэлектронных передатчиков; позволяет фиксировать отклонения импеданса линии от типового значения, при подключении к линии последовательно соединенных конденсатора с емкостью 100 пФ и более и резистора с сопротивлением 1 МОм; диапазон измерения токов утечки от 0.1 до 200 мА; диапазон измерения сопротивления изоляции от 100 кОм до 20 Мом; блокировку незаконно набранного номера и другое.

**2.2.4 Скрытие информации криптографическим методом**

Скрытие информации методом криптографического преобразования заключается в преобразовании ее составных частей (цифр, букв, слогов, слов) к неявному виду с помощью специальных алгоритмов и кодов ключей. Незащищенное конфиденциальное информационное сообщение зашифровывается и тем самым преобразуется в шифрограмму, т. е. в закрытый текст или графическое изображение документа. Для ознакомления с шифрограммой применяется обратный процесс: декодирование (дешифрование). Использование криптографии является одним из распространенных методов, значительно повышающих безопасность передачи данных хранящихся в удаленных устройствах памяти, а также при обмене информацией между удаленными пользователями и объектами.

Для шифрования обычно используется заданный алгоритм или устройство, реализующее данный алгоритм, который должен быть известен кругу лиц., для которого предназначается информация. Управление данного процесса шифрования осуществляется с помощью периодически меняющегося кода ключа, обеспечивающего каждый раз оригинальность представления информации при использовании одного и того же алгоритма. Знание секретного ключа дает возможность просто, надежно и быстро расшифровать информацию. Однако без ключа эта процедура может быть практически невыполнима даже при известном алгоритме шифрования.

Любое преобразование информации, даже самое простое, является очень эффективным средством, дающим возможность скрыть ее смысл от большинства неквалифицированных нарушителей.

Метод шифрования и кодирования использовались задолго до появления ЭВМ. Между кодированием и шифрованием нельзя провести отчетливой границы. В последнее время на практике слово "кодирование" применяют в целях цифрового представления информации при ее обработке на технических средствах, а "шифрование" -- при преобразовании информации в целях защиты от НСД. В данное время некоторые методы шифрования хорошо проработаны и являются основными. Для полного обеспечения защиты информации от НСД необходимо иметь представление о некоторых традиционных методах шифрования, таких как подстановка, перестановка, комбинированных и др.

Основные требования, предъявляемые к методам защитного преобразования:

- применяемый метод должен быть достаточно устойчивым к попыткам раскрыть исходный текст, имея только зашифрованный текст;

- объем ключа должен быть оптимальным для запоминания и пересылки;

- алгоритм преобразования информации и ключ, используемые для шифрования и дешифрования, не должны быть очень сложными: затраты на защитные преобразования должны быть приемлемы при определенном уровне сохранности информации;

- ошибки в шифровании не должны вызывать потерю информации. Из-за возникновения ошибок передачи обработанного сообщения по каналам связи не должна исключаться возможность надежной расшифровки текста у получателя;

- длина зашифрованного текста не должна превышать длину исходного текста;

- необходимые временные и финансовые затраты на шифрование и дешифрование информации должны определяются требуемой степенью защиты информации.

Перечисленные требования характерны в основном для традиционных средств защитных преобразований. С развитием устройств памяти, позволяющих с большей плотностью записывать и долгое время надежно хранить большие объемы информации, ограничение на объем используемого ключа может быть снижено. Появление и развитие электронных элементов позволили разработать недорогие устройства, обеспечивающие преобразование информации.

Однако в настоящее время скорость передачи информации пока еще значительно отстает от скорости ее обработки. В условиях применения ЭВМ, при существующей надежности аппаратуры и развитых методах обнаружения и исправления ошибок требование по достоверности информации на приемке, при возникновении ошибок стало менее актуально. Кроме того, технология передачи данных, принятая в сетях ЭВМ и АСУ, предусматривает повторную передачу защищенной информации в случае обнаружения ошибок передачи сообщения.

Множество современных методов защитных преобразований можно классифицировать на четыре большие группы:

I. перестановки - заключается в том, что входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов;

II. замены (подстановки) - заключаются в том, что символы исходного текста (блока), записанные в одном алфавите, заменяются символами другого алфавита в соответствии с принятым ключом преобразования;

III. аддитивные - в данном методе в качестве ключа используется некоторая последовательность букв того же алфавита и такой же длины, что и в исходном тексте. Шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите (для примера, если используется двоичный алфавит, то производится сложение по модулю два);

IV. комбинированные методы - могут содержать в себе основы нескольких методов.

Методы перестановки и подстановки характеризуются короткой длиной ключа, а надежность их защиты определяется сложностью алгоритмов преобразования.

Для аддитивных методов характерны простые алгоритмы преобразования, а их надежность основана на увеличении длины ключа.

Все перечисленные методы относятся к так называемому симметричному шифрованию: один и тот же ключ используется для шифрования и дешифрования.

В последнее время появились методы несимметричного шифрования:

один ключ для шифрования (открытый), второй -- для дешифрования (закрытый).

Принципиальное значение для надежности шифрования имеет отношение длины ключа к длине закрываемого им текста. Чем больше оно приближается к единице, тем надежнее шифрование. Но также нельзя забывать и про то, что это отношение распространяется не только на данное шифруемое сообщение, но и на все остальные, закрытые этим же кодом и передаваемые постоянно и периодически в течение времени существования данного ключа до замены новым значением.

**ЗАКЛЮЧЕНИЕ**

Проблема защиты информации появилась задолго до разработки компьютерной техники, а появление ЭВМ лишь перевело ее на новый уровень. И как показывает практика: лучшая защита от нападения это не допускать его. Нельзя защиту информации ограничивать только техническими методами. Основной недостаток защиты - это человеческий фактор и поэтому надежность системы безопасности зависит от отношения к ней.

Для поддержания защиты на высоком уровне необходимо постоянно совершенствоваться вместе с развитием современной техники и технологий, так сказать двигаться в ногу со временем.

**Список литературы**

**1.** Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. - М.: ООО «Издательство Машиностроение», 2009 - 508 с. Источник - http://window.edu.ru/window\_catalog/pdf2txt?p\_id=33810

2. Мельников В. Защита информации в компьютерных системах. М.: Финансы и статистика, Электронинформ, 1997 - 368 с.

3. http://kiev-security.org.ua/box/6/22.shtml

**Тема 10. Международные стандарты на системы управления информационной безопасностью.**

**1. Стандарты информационной безопасности:**

**Россия и мир**

Стандартизация является инструментом обеспечения качества продукции, работ и услуг - важного аспекта многогранной коммерческой деятельности.

Проблема качества актуальна для всех стран независимо от зрелости их рыночной экономики. Чтобы стать участником мирового хозяйства и международных экономических отношений необходимо совершенствование национальной экономики с учетом мировых достижений и тенденций.

Переход России к рыночной экономике определяет новые условия для деятельности отечественных фирм и промышленных предприятий. Право предприятий на самостоятельность не означает вседозволенность в решениях, а заставляет изучать, знать и применять в своей практике принятые во всем мире «правила игры». Международное сотрудничество по любым направлениям и на любом уровне требует гармонизации этих правил с международными и национальными нормами.

Стандартизация в том виде как это было в плановой экономике, не только не вписывалась в новые условия работы, но и тормозила либо просто делала невозможной интеграцию России в цивилизованное экономическое пространство. Особенно ярким примером служит тому условие вступления нашею государства в **ГАТТ/ВТО**.

За двадцать лет существования стандартов информационной безопасности в результате естественного отбора остались только основополагающие, которые досих пор претерпевают постоянные изменения.

Рынок ИБ России только сегодня начинает оправляться от «влияния гостайны», и в области стандартизации это особенно заметно.

Анализируя существующую сегодня в мире ситуацию в области стандартизации по информационной безопасности, за годы развития индустрии ИБ **можно выделить следующие временные периоды, название которых наиболее точным образом характеризует естественное развитие данного процесса:**

1.Появление стандартов (1988 — 1995 годы).

2. Испытание практикой (1996 — 2000).

3. Выживание сильнейших (2001— и до настоящего времени)

**Первый период** характеризовался естественным развитием информационных технологий, за которым с трудом поспевала наука и практика в области ИБ. В этот период формировался понятийный аппарат и основные подходы в области ИБ, вплоть до самых экзотических.

**Период конца 80-х и особенно начала 90-х годов** характеризовался появлением огромного числа различных стандартов в области ИБ.

Стандарты появлялись как у отдельных компаний, или консорциумов **(X-Open, Good Practice и т.д.)**, так и таких авторитетных институтов как **NIST (National Institute of Standards and Technologies**) и связка **BSI (British Standards Institute)** с **ISO (International Standards Organization).**

Отметим, **что NIST и BSI сегодня основные мировые конкуренты в области стандартизации.**

**Естественными недостатками стандартов этого периода** являлись:

- их слабая практическая проработка;

- и отсутствие единых подходов, единого понимания информационной безопасности.

Только время могло преодолеть эти недостатки. Что и случилось во втором и третьем периоде — практическое применение стандартов стимулировало их естественный отбор.

Период испытания практикой в середине 90-х плавно перешел в период естественного отбора и выживания сильнейших стандартов.

Очевидно, что область ИБ является достаточно замкнутой и ограниченной, поэтому нет никакого смысла иметь огромное число стандартов, которые, помимо всего прочего, пересекаются друг с другом и пытаются разными способами описать одну и туже предметную область.

На практике достаточно иметь несколько основополагающих стандартов, которые признаются большинством специалистов и которые используются бизнесом на практике.

Поэтому естественным образом в этой битве стандартов выживали и выжили только сильнейшие, например стандарт **ISO 15408**, регламентирующий требования по защищенности ПО, или стандарт управления **ISO 27001/17799**.

 **Эти стандарты сегодня получили статус международных**.

Правда, есть одно «но». Мир разделился на две географически независимые, с точки зрения стандартизации, зоны:

- **Европа и Азия признают стандарты ISO**,

- **а США предпочитает использовать стандарты NIST**.

Отметим малоизвестный факт, что многие из наиболее известных стандартов **ISO** вышли из недр **BSI**:

- ISO 17799,

- ISO 9001,

- ISO 14001.

**2. Российские особенности**

В России исторически все началось в начале 90-х годов с написания своих оригинальных стандартов в области ИБ, ориентированных прежде всего на защиту гостайны.

Эта российская особенность стандартизации являлась серьезным недостатком для бизнеса, так как подходы к защите гостайны и бизнес информации кардинально отличаются.

Основные недостатки такого подхода для бизнеса (а, скорее, полная его неприменимость) состояли в том, что:

1) в российских стандартах не учитывались такие важные угрозы бизнеса как доступность,

2) не применялся подход к построению системы защиты на основе анализа рисков,

3) отсутствовало само понятие и принципы функционирования системы управления ИБ.

При этом, важно отметить, что данные стандарты изначально для бизнеса и не предназначались.

**Просто на момент их создания не было понимания, что:**

- **во-первых**, они нужны российскому бизнес сообществу,

**- во-вторых,** как именно должен выглядеть бизнес-ориентированный стандарт, а других стандартов в РФ не было.

В отличие же от российских, известные нам западные стандарты, были, прежде всего, ориентированы на защиту бизнес информации, поэтому широко применялись на практике западным бизнес сообществом.

Исторически в РФ область информационной безопасности регулировалась государственными регуляторами и спецслужбами.

С течением времени стало очевидно, что проблема ИБ это не только проблема государственных органов, но и бизнеса, который в государстве с рыночной экономикой играет важнейшую роль.

 Это привело к тому, что в последние годы государством взят курс как на либерализацию рынка ИБ, так и на использование лучших бизнес ориентированных западных стандартов.

Первым шагом в этом направлении стало принятие **ГОСТ 15408;** следующие - **ГОСТ 17799** и **ГОСТ 27001**. Появление этих стандартов в ранге ГОСТ — осмысленный шаг, который в том числе призван показать ориентацию России на лучше западные стандарты при вступлении в **ВТО.**

В любом случае принятие и, что крайне важно, — использование на практике лучших западных стандартов (особенно **ISO 27001/17799)** благотворно скажется на защищенности как государственных объектов, так и бизнеса, так как сегодня вопрос обеспечения безопасности бизнеса часто становятся вопросом обеспечения безопасности государства.

Например, отток вкладчиков какого-либо крупного банка, вызванный информацией об успешной хакерской атаке, может привести к цепной реакции и временными проблемами для платежной системы всей страны.

В целом, можно отметить, что сегодня процесс принятия западных стандартов в России вышел на финальную стадию и в ближайшее время мы сможем констатировать наличие российских **ГОСТ-ов**, которые определяют требования к защищенному программному обеспечению (**ГОСТ 15408**), так и **ГОСТ-ов**, описывающих требования к системе управления информационной безопасностью (**ГОСТ 27001** и **ГОСТ 17799).**

Этот процесс должен привести как к повышению общего профессионального уровня в РФ в области обеспечения ИБ, так и к повышению

уровня защищенности и управляемости информационных систем государственных и бизнес структур.

**3. Стандарты**

Под стандартом понимается документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции,

правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг.

Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения.

Деятельность по установлению правил и характеристик в целях их добровольного многократного использования, на­правленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг, называется **стандартизацией.**

**Стандартизация осуществляется в следующих целях:**

* повышение уровня безопасности жизни или здоровья граждан, имущества физических или юридических лиц, государствен­ного или муниципального имущества, экологической безопасно­сти, безопасности жизни или здоровья животных и растений, содействие соблюдению требований технических регламентов;
* повышение уровня безопасности объектов с учетом риска
возникновения чрезвычайных ситуаций природного и техногенного характера;
* обеспечение научно-технического прогресса;
* повышение конкурентоспособности продукции, работ, услуг;
* рациональное использование ресурсов;
* техническая и информационная совместимость;
* сопоставимость результатов исследований (испытаний) и измерений, технических и экономико-статистических данных;
* взаимозаменяемость продукции.

Формальной причиной необходимости использования стандартов является то, что необходимость следования некоторым из них закреплена

законодательно.

Реальные причины гораздо глубже — обычно стандарт является результатом формализации опыта лучших специалистов в той или иной области, потому представляет собой надежный источник оптимальных и проверенных решений.

 **Стандарты являются также одним из основных механизмов обеспечения совместимости продуктов и систем — в частности, АС, использующих решения от различных производителей.**

**Стандартизация осуществляется в соответствии со следующими принципами:**

* добровольного применения стандартов;
* максимального учета при разработке стандартов законных ин­тересов заинтересованных лиц;
* применения международного стандарта как основы разработки национального стандарта, за исключением случаев, если такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям Российской Федерации, техническим и (или) технологическим особенностям или по иным основаниям либо Российская Федерация в соответствии с установленными

процедурами выступала против принятия международного стандарта или отдельного его положения;

* недопустимости создания препятствий производству и обращению продукции, выполнению работ и оказанию услуг в большей степени, чем это минимально необходимо для выполнения елей стандартизации;
* недопустимости установления таких стандартов, которые
противоречат техническим регламентам;
* обеспечения условий для единообразного применения стандартов.

**К документам в области стандартизации*,* используемым на**

**тер­ритории Российской Федерации, относятся:**

* национальные стандарты;
* правила стандартизации, нормы и рекомендации в области стандартизации;
* применяемые в установленном порядке классификации, общероссийские классификаторы технико-экономической и социальной

информации;

* стандарты организаций.

**4. Национальная система стандартизации***.*

Национальные стандарты и общероссийские классификаторы технико-экономической и социальной информации, в том числе правила их разработки и применения, представляют собой **национальную систему стандартизации***.*

**Национальный стандарт**применяется на добровольной основе равным образом и в равной мере независимо от страны и (или) места происхождения

продукции, осуществления процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ и оказания услуг, видов или особенностей сделок и (или) лиц, являющихся изготовителями, исполнителями, продавцами, приобретателями.

Применение национального стандарта подтверждается знаком соответствия национальному стандарту. Разработчиком национального стандарта может быть любое лицо.

**Общероссийские классификаторы технико-экономической и соци­альной информации**(далее — **общероссийские классификаторы**) — это нормативные документы, распределяющие технико-экономическую и социальную информацию в соответствии с ее классификацией (классами,

группами, видами и другим) и являющиеся обязательными для применения при создании государственных информационных систем и информационных ресурсов и межведомственном обмене информацией.

Порядок разработки, принятия, введения в действие, ведения и применения общероссийских классификаторов в социально-экономической области (в том числе в области прогнозирования, статистического учета,

банковской деятельности, налогообложения, при межведомственном информационном обмене, создании информационных систем и информационных ресурсов) **устанавливается Правительством Российской Федерации.**

**Стандарты организаций *,*** в том числе коммерческих, общественных,

научных, саморегулируемых, объединений юридических лиц, могут разрабатываться и утверждаться ими самостоятельно, исходя из необходимости применения их для целей стандартизации, для совершенствования производства и обеспечения качества продукции, выполнения работ, оказания услуг, а также для распространения и использования полученных в различных областях знаний результатов исследований (испытаний), измерений и

разработок.

**Стандарты организаций** применяются равным образом и в равной мере независимо от страны и (или) места происхождения продукции, осуществления процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ и оказания услуг

**5. Стандарты в области информационной безопасности РФ**

В современном мире нормативно-правовая база должна быть

согласована с международной практикой. Назрела необходимость приведения российских стандартов и сертификационных нормативов в соответствие с

международным уровнем ИТ вообще и по критериям оценки безопасности информационных технологий в частности.

**Этому есть две сновные причины**:

* необходимость защищенного взаимодействия с зарубежными
организациями и зарубежными филиалами российских
организаций;
* доминирование аппаратно-программных продуктов зарубежного
производства.

Обеспечение безопасности ИТ невозможно без разработки соответствующих законодательных актов и нормативно-технических документов. Новые критерии оценки безопасности информационных технологий занимают среди них особое место. Только стандартизованные отечественные критерии позволяют проводить сравнительный анализ и сопоставимую оценку продуктов ИТ.

В«**Доктрине информационной безопасности Российской Федерации**», утверждённой Президентом 09.09.2000г., одной из составляющих национальных интересов России в информационной сфере определена защита информационных ресурсов от несанкционированного доступа и обеспечение безопасности информационных и телекоммуникационных систем.

**К числу важнейших задач, поставленных в Доктрине, относятся:**

* согласование отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления, информационных и телекоммуникационных систем общего и специального назначения;
* разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности
* разработка методов и средств обеспечения информационной

безопасности Российской Федерации на основе единых требований и подходов.

Решение этих задач связано, прежде всего, с развитием нормативно-методической базы обеспечения безопасности информационных технологий (ИТ).

Исторически сложилось, что в России проблемы безопасности ИТ изучались и своевременно решались только в сфере охраны государственной тайны. Аналогичные, но имеющие собственную специфику задачи коммерческого сектора экономики долгое время не находили соответствующих решений. Данный факт до сих пор существенно замедляет появление и развитие безопасных ИТ-средств на отечественном рынке, который интегрируется с мировой системой. Тем более что у защиты информации *в* коммерческой автоматизированной системе есть свои особенности, которые просто необходимо учитывать, ведь они оказывают серьезное влияние на технологию информационной безопасности.

**Перечислим основные из них** :

1. Приоритет экономических факторов. Для коммерческой
автоматизированной системы очень важно снизить либо исключить финансовые потери и обеспечить получение прибыли владельцем и
пользователями данного инструментария в условиях реальных рисков.
Важным условием при этом, в частности, является минимизация типично банковских рисков (например, потерь за счет ошибочных направлений платежей, фальсификации платежных документов и т.п.);
2. Открытость проектирования, предусматривающая создание
подсистемы защиты информации из средств, широко доступных на рынке и работающих в открытых системах;
3. Юридическая значимость коммерческой информации, которую можно
определить как свойство безопасной информации, позволяющее обеспечить юридическую силу электронным документам или информационным процессам в соответствии с правовым режимом информационных ресурсов,

установленным законодательством Российской Федерации. Это условие в последнее время приобретает все большую значимость в нашей стране наряду с созданием нормативно-правовой базы безопасности **ИТ** (особенно при
взаимодействии автоматизированных систем разных юридических лиц).

Очевидно, что создание безопасных **ИТ**, обрабатывающих конфиденциальную информацию, не содержащую государственной тайны, исключительно важно для экономико-финансовой жизни современной России.

**Применение в России гармонизированного стандарта ISO 15408 ("Соmmon Сriteriа"), отражающего новейшие мировые достижения оценки информационной безопасности, позволит:**

* приобщить российские ИТ к современным международным
требованиям по информационной безопасности, что упростит,
например, применение зарубежной продукции и экспорт собственной;
* облегчить разработку соответствующих российских
специализированных нормативно-методических материалов для
испытаний, оценки (контроля) и сертификации средств и систем
безопасных банковских и других ИТ;
* создать основу для качественной и количественной оценки
информационных рисков, необходимую при страховании
автоматизированных систем;
* снизить общие расходы на поддержание режима информационной
безопасности в банках и корпорациях за счет типизации и
унификации методов, мер и средств защиты информации.

В настоящее время в России наряду с отечественной нормативной базой широко используются около **140 международных стандартов** в области информационных технологий. Из них **около 30 затрагивают вопросы защиты** информации.

Некоторые международные стандарты по защите информации приняты и введены в действие в России, но эти стандарты не составляют целостной основы для решения проблем информационной безопасности, особенно в части нормативного регулирования, методического и инструментального обеспечения разработки, оценки и сертификации безопасности ИТ с учетом современного уровня развития, масштабов и многообразия угроз.

Общепринятая классификация с**тандартов в области информацион­ной безопасности** с примерами приведена на рисунке.

|  |
| --- |
| **Стандарты в области информационной безопасности**  |
| **Оценочные стандарты** | **Спецификации** |
| Предназначены для оценки и классификации автоматизированных систем и средств защиты информации по требованиям безопасности | Регламентируют различные аспекты реализации и использования средств и методов защиты |
| «**Оранжевая книга**» | **Х.509** – инфраструктура открытых ключей |
| РД Гостехкомиссии России | **ГОСТ 28147-89** – симметричный криптографический алгоритм |
| «**Общие критерии**» | Управленческие стандарты (**ISO17799, ISO 27001** и др.) |

Рис.1. Классификация стандартов в области информационной безопасности

Перечислим основные стандарты в области информа­ционной безопасности, имеющие в настоящее время офи­циальный статус в Российской Федерации:

**6. Руководящие документы (РД) Гостехкомиссии России**

**Гостехкомиссия России (ныне это Федеральная служба по техническому и экспортному контролю — ФСТЭК России)** в период с 1992 по 1999 г. разработала пакет руководящих документов, посвященных вопросам защи­ты информации в автоматизированных системах.

**Наибольшее практическое значение представляют следующие документы:**

1. Защита от несанкционированного доступа к инфор­мации. Термины и определения .
2. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционирован­ного доступа к информации .
3. Автоматизированные системы. Защита от несанкцио­нированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
4. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
5. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа.
6. Показатели защищенности от несанкционированного доступа к информации.
7. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.

**Третий и четвёртый документы были опубликованы в 1992г**. В них излагались требования к обеспечению защиты компьютерных систем в соответствии с аналогичными требованиями «Оранжевой книги».

В документе: « **Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»** рассматриваются требования к обеспечению защищенности отдельных программно-аппаратных элементов защищенных компьютерных систем. Установлено семь классов защищенности средств вычислительной техники. Самые низкие требования предъявляют к классу 7, самые высокие - к первому классу. Требования этих классов в основном соответствуют аналогичным требованиям «**Оранжевой книги»,** при этом класс 7 соответствует классу 01 «Оранжевой книги», класс 6- классу С1, ....класс 1-классу А1.

**Второй документ, касающейся автоматизированных систем**: Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» - вводит стандарты защищенности не отдельных программно-аппаратных средств защиты, а всей защищенной компьютерной системы в целом. Система стандартов этого документа более существенно отличается от аналогичных стандартов Оранжевой книги.

Все автоматизированные системы разделяются на три группы, в каждой из которых вводится своя иерархия классов защиты. Всего вводится девять классов защиты.

В целом, отличия требований от требований в наиболее распространённом

диапазоне защищённости операционных систем по «Оранжевой книге» и по документам ФСТЭК ( Гостехкомиссии) незначительны.

**7. «Общие критерии». Криптографические стандарты. Управленческие стандарты**

 **«Общие критерии».**

Стандарт **ГОСТ Р ИСО/МЭК 15408-2002*,*** более изве­стный как «**Общие критерии*»,*** действует и приме­няется при проведении сертификации средств защи­ты, не предназначенных для работы с информацией, составляющей государственную тайну. В перспективе предполагается отказ от РД Гостехкомиссии России и полноценный переход к «Общим критериям» как еди­ному оценочному стандарту.

**Криптографические стандарты**

**(ГОСТ 28147-89, ГОСТ 3410-2001, ГОСТ 3411-94)** являются обязательными для применения в системах защиты информа­ции, позиционируемых как средства криптографиче­ской защиты.

**Управленческие стандарты**

**ISO 17799-2005 и ISО 27001-2005** в настоящее время не имеют в РФ офици­ального статуса, однако планируются к принятию в качестве ГОСТ в ближайшее время.

 Все остальные спецификации носят сугубо доброволь­ный характер, однако активно используются при постро­ении реальных систем, в первую очередь — в целях обес­печения их взаимной совместимости.

Как для «**Оранжевой книги**», так и для аналогич­ных ей руководящих документов Гостехкомиссии Рос­сии, характерны многочисленные недостатки.

**Наиболее существенные из них:**

* Документы ориентированы на обеспечение защиты информации от угроз
* нарушения конфиденциально­сти и, в определенной степени, целостности. Угрозы нарушения доступности практически не рассматри­ваются.
* Используемый «**табличны**й» подход не позволяет учесть специфику конкретных систем или продуктов, в том числе порядок обработки информации в автоматизированной системе. Так, например, понятие «**политика безопасности**» в **РД ФСТЭК** не упоминается.
* Документы содержат перечень механизмов, наличие которых необходимо для отнесения СВТ или АС к тому или иному классу защищенности. При этом совершен­но не формализованы методы проверки корректности и адекватности реализации функциональных требо­ваний.
* Формулировки ряда требований чрезвычайно туман­ны и допускают неоднозначную интерпретацию.

В целом, **РД ФСТЭК** и **«Оранжевая книга»,** как и все другие оценочные стандарты первого поколения, создавались для давно ушедшей в прошлое материально-технической базы и по целому ряду аспек­тов являются морально устаревшими.

**8. Международный стандарт ИСО/МЭК 15408-99 «Критерии оценки безопасности информационных технологий» - «Общие критерии»**

Одним из направлений развития нормативно-методической базы обеспечения безопасности информационных технологий является внедрение в России **международного стандарта ИСО/МЭК 15408-99 «Критерии оценки безопасности информационных технологий».**

**8.1. Истоки и стимулы принятия**

Годом рождения стандарта можно считать 1990-й - именно тогда были начаты работы по созданию стандарта в области оценки безопасности информационных технологий (ИТ) под эгидой Международной организации по стандартизации (ИСО). Этот документ и был переведен и взят за основу при разработке **ГОСТ Р 15408-2002**

 Стандарт **ISО/IЕС 15408-1999 «Соттоп Сгiteria fог Information Тесhnolodgy Security Еvalution»**был раз­работан при содействии государственных организаций по стандартизации США, Канады, Великобритании, Франции, Германии и Голландии и унификация различных национальных стандартов в области оценки безопасности ИТ в период с 1990 по 1999 г. Развитие стандарта не­прерывно продолжается. Исторически за стандартом за­крепилось разговорное название **«Соттоп Сгiteria» — «Общие критерии».**

Разработчики стандарта преследовали следующие концептуальные цели:

* Сокращение затрат на оценку безопасности ИТ на основе взаимного
признания сертификатов.
* Унификация различных национальных стандартов в области оценки безопасности.
* Повышение уровня доверия к оценке безопасности ИТ

Заметим также, что спецификации стандарта обобщили основные положения и опыт использования "**Оранжевой книги**" и ее интерпретаций,

развили оценочные уровни доверия Европейских критериев, воплотили концепцию типовых профилей защиты Федеральных критериев США. Именно потому стандарт и получил название "**Общие критерии" (ОК**). Первая его версия

датирована январем 1996 г., в мае 1998 г. появляется вторая версия ОК, и, наконец, в июне 1999 г. был принят **международный стандарт ИСО/МЭК 15408**

Следует подчеркнуть, что положения **ОК** имеют достаточно обобщенный характер. По сути, **"Общие критерии"**  не содержат определенных требований к

конкретным системам защиты информации, а представляют собой некий набор определений и правил, рамках которых можно описывать различные системы защиты. На основе **ОК** потребитель может сам оценить встроенные в приобретаемое **ПО** механизмы защиты и их достаточность для его нужд. Документ полезен и **как руководство при разработке, причем не только специализированных средств защиты, но и любого ПО или аппаратных средств с функциями безопасности.**

В России аутентичный перевод «**Общих критериев» версии 2.0** принят в качестве **ГОСТ в 2002 г.** и **введен в действие с 1 января 2004** г. Точное название докумен­та **— ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопас­ности. Критерии оценки безопасности информацион­ных технологий»** ипредставляет собой точный перевод международного стандарта**.**

**Он принят постановлением Госстандарта России от 4.04.2002 г. № 133-ст с датой введения в действие 1 января 2004 г**.

 Заметим, что появление этого ГОСТ отражает не только процесс совершенствования российских стандартов с использованием международного опыта, но и часть правительственной программы по вступлению России в ВТО (как известно, при вступлении в эту организацию в стране-претенденте должны быть унифицированы пошлины, налоги, стандарты на производство, стандарты

качества и некоторые стандарты в области информационной безопасности).

**"Общие критерии"** заставляют отказаться от привычного нам представления, что функции защиты реализуют только специализированные средства. Общаясь на одном для всех языке **ОК**, **производители и потребители любого ПО смогут оценить, насколько используемые в нем механизмы**

**защиты отвечают требованиям политики безопасности организации.**

Кроме того, аудиторы, контролирующие адекватность мер безопасности, а также сотрудники уполномоченных органов, проводящих

аттестацию систем ИТ, смогут **оценивать выполнение требований по безопасности не отдельных компонентов, а системы в целом, причем в конкретной среде ее функционирования.**

**Документ состоит из трех частей :**

1. Введение и общая модель.

2. Функциональные требования безопасности.

1. Требования доверия к безопасности.

В перспективе «**Общие критерии**» должны заменить **РД Гостехкомиссии России** во всех системах сертифика­ции средств защиты информации. В настоящий момент оба поколения стандартов используются одновременно, причем «Общие критерии» применяются исключительно при проведении сертификации продуктов, не предназна­ченных для обработки информации, составляющей госу­дарственную тайну.

**8.2. Основные понятия «Общих критериев»**

Если попытаться кратко сформулировать **главную концепцию** "**Общих критериев"**, то, скорее всего, она будет выглядеть как "**угрозы и профили**". Окружающий нас мир не просто не идеален, он опасен. И эксплуатируемые в нем комплексные системы и ПО буквально со всех сторон окружают угрозы. В зависимости от того, в каких условиях эксплуатируется конкретный ИТ-объект (например, подключена ли данная система к сетям общего пользования или функционирует автономно), к нему можно предъявить столь же конкретный перечень требований к защите, т е. формализовать так называемый профиль

защиты. Такие требования могут быть сформулированы пользователем в техническом задании на разработку или сформированы самостоятельно создателем системы или средства. В процессе сертификации некой системы по ОК сертифицирующий орган рассматривает документ, который называется "задание по безопасности", - представляемый разработчиком системы в органы сертификации перечень требований к данной системе по безопасности. Сертификат подтверждает факт наличия в системе функционала, выполняющего заявленные требования по безопасности.

Основное свойство «**Общих критериев» (ОК**) — это максимально возможная **универсальность.**

**Под объектом оценки** (ОО) понимается произвольный продукт информа­ционных технологий или система с руководствами адми­нистратора и пользователя.

**Продукт**рассматривается как совокупность программных, программно-аппаратных или аппаратных средств информационных технологий, предо­ставляющая определенные функциональные возможнос­ти и предназначенная для непосредственного использования или включения в состав различных систем.

В свою очередь, **система**— это специфическое воплощение ин­формационных технологий с конкретным назначением и условиями эксплуатации.

**Предполагается, что общие критерии могут быть использованы** **следующими** **категориями пользователей:**

**1. Потребители.**

ОК позволяют определить, вполне ли оцениваемый продукт или система удовлетворяют их потребностям в безопасности.

**2. Разработчики.**

Конструкции ОК могут быть использованы для формирования

утверждения о соответствии объекта оценки установленным требованиям.

**3. Оценщики.**

Стандарт может быть использован при формировании заключения о соответствии ОО предъявляемым к ним требованиям безопасности.

**Объект оценки** рассматривается в контексте **среды безопасности,** в которую включаются:

* **законодательная среда *-*** законы и нормативные акты, затрагивающие ОО;
* **административная среда**— положения политик безопасности, затрагивающих ОО и учитывающих его особенности;
* **процедурная среда**— меры физической защиты, персонал и его специфика;
* **программно-техническая среда**— назначение ОО, предполагаемые области его применения.

**При подготовке к оценке формализуются следующие** **аспекты среды ОО:**

**1. Предположения безопасности**Предположения выделяют ОО из общего контекста и задают границы его рассмотрения. Предполагается, что среда ОО удовлетворяет данным предположениям. При проведении оценки предположения безопасности прини­маются без доказательств.

**2. Угрозы безопасности**

Выделяются угрозы, наличие которых в рассматриваемой среде установлено или предполагается.

**Угроза характеризуется следующими параметрами:**

* источник угрозы;
* предполагаемый способ реализации угрозы;
* уязвимости, которые являются предпосылкой для реализации угрозы;
* активы, которые являются целью нападения;
* нарушаемые свойства безопасности активов;
* возможные последствия реализации угрозы.

**3. Политики безопасности**

Излагаются положения политики безопасности, применяемые в организации, которые имеют непосредственное отношение к ОО.

На основании сформулированных предположений безопасности, при учете угроз и политик формулируются **цели безопасности**для ОО, направленные на обеспечение противостояния угрозам и выполнение положений политики безопасности.

Для достижения поставленных целей к ОО и его среде предъявляются **требования безопасности.**

**Вторая и третья части «Общих критериев**» представляют собой каталоги требований безопасности следующих типов:

* **Функциональные требования**(**Часть 2)** — соответ­ствуют активному аспекту защиты и предъявляются к функциям безопасности ОО и реализующим их ме­ханизмам.
* **Требования доверия**(**Часть 3**) — предъявляются к технологии и процессу разработки, эксплуатации и оценки ОО и призваны гарантировать адекватность реализации механизмов безопасности.

При формулировании требований к ОО могут быть разработаны два

документа:

**1.Профиль защиты**— не зависящая от конкретной реализации совокупность требований информационных технологий для некоторой категории **ОО**. Профиль защиты (**ПЗ**) не привязан к конкретному **ОО** и представляет собой обобщенный стандартный набор функциональных требований и требований доверия

для определенного класса продуктов или систем. Например, может быть разработан профиль защиты на межсетевой экран корпоративного уровня или на биллинговую систему.

**Биллинговая** **система** (БС) — это бухгалтерская **система**, программное обеспечение, иными словами — «софт», разработанный специально для операторов.

**Биллинг в электросвязи** — комплекс процессов и решений на предприятиях связи, ответственных за сбор информации об использовании телекоммуникационных услуг, их тарификацию, выставление счетов абонентам, обработку платежей.

**Биллинговая** **система** — прикладное программное обеспечение поддержки...

**Биллинговая** **система** - программный комплекс, осуществляющий учет объема потребляемых абонентами услуг, расчет и списание денежных средств в...

Именно каталог утвержденных профилей защиты должен послужить

заменой традиционных руководящих документов **ФСТЭК.**

**2. Задание по безопасности—** документ, содержа­щий требования безопасности для конкретного ОО и специфицирующий функции безопасности и меры доверия, предлагаемые объектом оценки для выполнения установ­ленных требований. В задании по безопасности (**ЗБ**) мо­жет быть заявлено соответствие одному или нескольким профилям защиты.

**ЗБ** можно рассматривать как техническое задание на подсистему обеспечения информационной безопасности для **ОО.**

Задание по безопасности служит основой для проведе­ния оценки **ОО** с целью демонстрации соответствия его требованиям безопасности.

По сравнению с традиционными стандартами «**Общие критерии**» представляют собой принципиально более гибкий и универсальный инстру­мент.

**Однако стандарт не претендует на всеобъемлющую универсальность и, в частности, имеет следующие ограничения:**

1. **ОК не содержат критериев оценки**, касающихся администрирования механизмов безопасности, непосредственно не относящихся к мерам безопасности информационных технологий (управление персоналом, вопросы физической безопасности и т.д.). Соответствующие аспекты в рамках «**Общих критериев**» могут рассматриваться исключительно в виде предположений безопасности. Предполагается, что оценка соответствующих механизмов должна проводиться с использованием других стандартов.
2. **Вопросы защиты информации от утечки по техническим каналам**, такие как контроль **ПЭМИН**, непосредственно не затрагиваются, хотя многие концепции ОК потенциально применимы и в данной области.
3. **В ОК не рассматриваются** методология оценки, и административно-правовая структура, в рамках которой критерии могут применяться органами оценки.
4. **Процедуры использования** результатов оценки при аттестации
5. продуктов и систем находятся вне области действия **ОК.**
6. **В ОК не входят критерии оценки** специфических свойств криптографических алгоритмов. Независимая оценка математических свойств криптографических компонентов, встроенных в **ОО**, должна проводиться как

самостоятельная независимая процедура.

**9. Выводы по применению в РФ международного стандарта ISО 15408**

Необходимо констатировать следующее. Несмотря на то, что принят новый **ГОСТ/ИСО-МЭК,** Россия не спешит с ратификацией соглашения о вступлении в сообщество государств, признавших действие международного стандарта **ISО 15408**. Внедрение его отечественной версии "для внутреннего

пользования" выхолащивает практический смысл сделанной работы. Это означает, что в России по-прежнему требуется **повторное подтверждение надежности сертифицированных за границей средств информационной безопасности.** Аналогично,.российским разработкам, сертифицированным по ГОСТ/ИСО МЭК 15408-2002, в случае их применения иностранными компаниями, требуется **повторное подтверждение надежности сертифицированных за границей средств информационной безопасности.** .

Кроме того, **стандарт ориентирован прежде всего на достаточно крупные, комплексные системы**.

Применение **стандарта ISО 15408** к конкретным подсистемам ИБ, по примеру того, как это делалось в РД, не совсем корректно. Отдельные вопросы вызывает также декларированная в "Общих критериях" система доверия, начальный уровень которой практически подразумевает лишь то, что некоторые механизмы обеспечения безопасности определены в "Руководстве администратора":

**10 Обзор международных стандартов в области информационной безопасности, принятых в РФ**

Международные стандарты позволяют дополнить отечественное законодательство в тех областях, которые не затрагиваются российскими нормативно-правовыми документами. Примерами таких областей является аудит информационной безопасности, интеграция различных средств обеспечения безопасности, управление системами защиты и др. В отличие от положений российского законодательства, требования международных стандартов носят рекомендательный характер.

**В настоящее время на территории России наибольшее распространение получили следующие международные стандарты**:

* **стандарт ISO / IEC 17799** "Информационная технология. Система менеджмента информационной безопасности. Требования";
* **стандарт ISO / IEC 27001** "Информационная технология. Методы обеспечения безопасности. Руководство по управлению информационной безопасностью".
* **стандарт CobiT** ( Control Objectives for Information and related Technology, "Контрольные Объекты для Информационной и смежных Технологий");
* **стандарт ITIL** ( Information Technologies Infrastructure Library, "Библиотека инфраструктуры информационных технологий");
* методика проведения аудита информационной безопасности OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation, "Методика оценки критических угроз, информационных активов и уязвимостей").

**Международный стандарт ISO / IEC 17799** представляет собой набор рекомендаций по применению организационно-технических мер безопасности для эффективной защиты автоматизированных систем.

В **2007 г. ISO / IEC 17799 был принят в качестве ГОСТа.**

Стандарт состоит из одиннадцати разделов, каждый из которых описывает одну из областей информационной безопасности.

Краткое описание разделов стандарта **ISO / IEC 17799** приведено в [табл. 1](http://www.intuit.ru/studies/courses/600/456/lecture/10227?page=3#table.29.1).

|  |
| --- |
| **Таблица .1. Краткое описание разделов стандарта ISO/IEC 17799** |
| **№**  | **Раздел стандарта**  | **Описание раздела**  |
| **1** | "Политика информационной безопасности" | Раздел стандарта определяет требования к структуре политики информационной безопасности организации, а также к правилам ее последующего анализа и пересмотра. В соответствии с рекомендациями стандарта политика должна включать в себя описание мер защиты от информационных атак злоумышленников  |
| **2** | "Организационные меры защиты" | Раздел содержит рекомендации в части проведения внутренних совещаний по вопросам информационной безопасности, аутсорсинга консалтинговых услуг по безопасности, а также рекомендации по соблюдению мер защиты при предоставлении доступа сторонним организациям к ресурсам автоматизированной системы  |
| **3** | "Безопасность персонала" | Раздел включает в себя рекомендации по мерам безопасности, которые необходимо предпринять при приеме сотрудников на работу, а также рекомендации по обучению сотрудников вопросам безопасности и способам регистрации сведений о выявленных инцидентах. При этом в качестве возможных инцидентов в рамках стандарта рассматриваются события, связанные в том числе с выявлением информационных атак  |
| **4** | "Классификация и управление информационными ресурсами" | В разделе определены типы ресурсов и операций над ними, которые должны подлежать обязательной инвентаризации и последующей классификации по требуемому уровню защиты |
| **5** | "Физическая безопасность" | В разделе описаны рекомендации по защите физического периметра организации, а также помещений, оборудования и каналов связи |
| **6** | "Управление коммуникациями и информационными процессами" | В разделе приведены рекомендации: по составлению должностных инструкций персонала, ответственного за обеспечение безопасности; по анализу инцидентов, связанных с нарушением информационной безопасности; по защите от вирусов и другого вредоносного программного обеспечения; по резервному копированию информационных ресурсов; по защите сетевого взаимодействия между узлами системы; по обеспечению безопасности съемных носителей информации |
| **7** | "Контроль доступа" | Раздел содержит рекомендации по управлению правами доступа пользователей к информационным, программным и аппаратным ресурсам организации. Приведены также рекомендации по мониторингу операций доступа к информационным ресурсам |
| **8** | "Разработка, сопровождение и приобретение автоматизированной системы" | В разделе описаны рекомендации по применению различных средств защиты на технологическом и эксплуатационном этапе жизненного цикла автоматизированной системы. Так, например, данный раздел включает в себя рекомендации по защите от информационных атак злоумышленников. В отличие от предыдущей версии стандарта в редакции 2005 г. определены требования безопасности, которые необходимо соблюдать не только при разработке, но и в случае приобретения готовой информационной системы  |
| **9** | "Управление инцидентами в области информационной безопасности" | Раздел содержит требования по правилу сбора и обработки информации о событиях, связанных с возможным нарушением информационной безопасности компании. В разделе также определены требования к сбору доказательной базы, необходимой для расследования возможных инцидентов |
| **10** | "Управление непрерывностью ведения бизнеса" | Раздел включает в себя рекомендации по созданию и реализации плана обеспечения непрерывности бизнес-процесса. Данный план описывает те действия, которые должны проводиться в организации в случае возникновения нештатных или аварийных ситуаций |
| **11** | "Соответствие требованиям и стандартам" | В разделе приводятся рекомендации по соблюдению авторских прав на использование программного обеспечения, а также местного законодательства в области защиты информации  |



**Рис. 2.** Модель процесса управления информационной безопасностью

**Международный стандарт ISO / IEC 27001** описывает требования к системе управления информационной безопасностью ISMS ( information security management system ). Стандарт базируется на процессном подходе, предполагающем непрерывность выполнения работ по поддержанию должного уровня информационной безопасности. **ISO / IEC 27001** базируется на модели **PDCA ( Plan Do Check Act** ), предусматривающей внедрение процесса управления, состоящего из четырех базовых этапов ([рис.](http://www.intuit.ru/studies/courses/600/456/lecture/10227?page=3#image.29.2) 2):

1. **Этап планирования,**на котором проводится анализ и оценка рисков информационной безопасности компании.
2. **Этап реализации**,в рамках которого осуществляется разработка плана минимизации рисков, реализуются программы по обучению и осведомленности персонала, создаются необходимые документы и др.
3. **Этап проверки**,на котором проводится мониторинг и контроль работы средств защиты АС, проводится аудит информационной безопасности, а также повторная оценка рисков. На данном этапе осуществляется разработка рекомендаций по совершенствованию системы мер защиты информации.
4. **Этап совершенствования**,предполагающего внесение изменений в существующие меры по защиты информации с целью повышения их эффективности.

**Стандарт CobiT** разработан международной ассоциацией **ISACA** и предназначен для обеспечения эффективного управления информационными технологиями (ИТ) с точки зрения целей и задач бизнес-процессов компании. Согласно **CobiT** повышение эффективности управления ИТ позволяет увеличить отдачу от инвестиций в инфокоммуникационные системы, а также повысить конкурентоспособность предприятия. В соответствии с этим стандартом все ИТ-ресурсы компании должны эффективно управляться определенными ИТ-процессами, что позволит обеспечить своевременное предоставление информации, необходимой организации для достижения ее бизнес-целей. В стандарте **CobiT** определено тридцать четыре ИТ-процесса, сгруппированных в четыре домена: "планирование и организация", "проектирование и внедрение", "эксплуатация и сопровождение", и "мониторинг". Каждый из этих процессов описывается совокупностью показателей, на основе которых осуществляется оценка эффективности существующих механизмов управления ИТ-ресурсами.

Оценка осуществляется по шестибалльной шкале, где каждый уровень соответствует определенной степени "зрелости" процессов управления ИТ.

В соответствии с **CobiT ИТ**-ресурсы могут включать в себя: данные, приложения, технологии, оборудование и людские ресурсы. Стандарт **CobiT** определяет следующие критерии, по которым возможно проведение оценки информационных ресурсов, участвующих в бизнес-процессах организации:

* эффективность - актуальность информации, гарантирующая своевременное получение корректных данных, необходимых для бизнес-процессов компании;
* продуктивность - обеспечение доступности информации с помощью оптимального использования имеющихся ИТ-ресурсов;
* конфиденциальность - обеспечение защиты информации от несанкционированного доступа;
* целостность - точность, полнота и достоверность информации в соответствии с требованиями бизнеса;
* доступность - обеспечение своевременного доступа к информации в соответствии с требованиями бизнес-процессов;
* согласованность - соответствие информационных ресурсов законодательству, а также существующим договорным обязательствам;
* надежность - обеспечение доступа руководства организации к соответствующей информации, необходимой и достаточной для адекватного выполнения бизнес-процессов, создания объективных финансовых отчетов и т. д.

Один из **ИТ-процессов**, определенных в домене как "**эксплуатация и сопровождение"**, направлен на обеспечение комплексной информационной безопасности. В рамках этого процесса, в качестве одной из обязательных мер защиты, определена необходимость применения организационных и программно-технических средств информационной безопасности.

**Стандарт ITIL** представляет собой набор рекомендаций по управлению ИТ, разработанных Отделом Правительственной Торговли Великобритании ( United Kingdom's Office Of Government Commerce, OGC ).

**Стандарт рассматривает информационные технологии в виде сервисов, которые предоставляются внутри организации**.

Стандарт состоит из следующих **семи основных частей**, каждая из которых описывает один из **аспектов управления ИТ-сервисами**:

1. "Предоставление и поддержка ИТ-сервисов" ( Service support and delivery)
2. "Планирование внедрения процесса управления ИТ-услугами" ( Planning to implement service management ),
3. "Управление приложениями" ( Application management ),
4. "Управление инфраструктурой" ( Infrastructure management ),
5. "Управление безопасностью" ( Security management )
6. "Бизнес-перспектива" ( The business perspective ).

**Практическое внедрение стандарта ITIL направлено на достижение следующих целей:**

* увеличение качества предоставления ИТ-сервисов потребителям;
* снижение затрат на разработку и внедрение ИТ-сервисов внутри организации;
* улучшение взаимодействия и обмена информацией между пользователями и подразделениями организации, отвечающими за информационные технологии и безопасность;
* формализация процесса управления информационными ресурсами компании;
* обеспечение оптимального использования навыков и опыта, имеющегося у технических специалистов компании.

Раздел **ITIL "Управление безопасностью"** включает в себя рекомендации по созданию комплексной системы защиты предприятия. Согласно стандарту ITIL такая система должна сочетать в себе организационные и технические меры защиты информации. При этом в стандарте указывается, что в состав системы обеспечения информационной безопасности должны входить средства обнаружения и предотвращения атак.

**Стандарт ITIL дополняет CobiT,** поскольку он в большей мере ориентирован на технических специалистов и содержит больше информации по фактической реализации на практике положений этого стандарта.

**Методика проведения аудита информационной безопасности OCTAVE** разработана координационным центром немедленного реагирования CERT ( Computer Emergency Response Team ) и **предназначена для анализа уровня защищенности автоматизированных систем посредством оценки рисков.**

**Согласно этой методике процедура оценки рисков безопасности включает в себя три фазы:**

1. **Первая фаза**. В процессе реализации первой фазы формируется множество защищаемых ресурсов, в число которых может входить аппаратное и программное обеспечение, а также информационные ресурсы. Первая фаза оценки рисков проводится посредством интервьюирования административного и технического персонала организации, в введении которой находится обследуемая автоматизированная система. В процессе интервьюирования сотрудникам компании задается ряд вопросов, на основе которых рабочая группа, проводящая оценку рисков, составляет перечень защищаемых ресурсов и профили атак. Вместо интервьюирования может быть проведен анализ существующей организационно-технической документации, касающейся вопросов информационной безопасности.

2. **Вторая фаза**. Для каждого из защищаемых ресурсов создается профиль угроз, который описывает возможные сценарии проведения атаки.

**Профиль предусматривает следующие типы источников атаки:**

* несанкционированные действия внутренних или внешних пользователей АС;
* системные проблемы, связанные с дефектами аппаратного обеспечения или сбоями программного обеспечения;
* физические процессы или стихийные бедствия, например, землетрясения или наводнения.

В профиле также указывается тип возможного последствия, к которому может привести успешная реализация атаки - искажение ресурса, уничтожение ресурса, блокирование доступа к ресурсу или нарушение конфиденциальности ресурса.

Согласно методике **OCTAVE** в процессе реализации второй фазы определяется список программно-аппаратного обеспечения, которое применяется для хранения или обработки защищаемой информации. Далее проводится анализ защищенности этого программно-аппаратного комплекса с целью выявления имеющихся уязвимостей. Данная процедура реализуется при помощи специализированного программного обеспечения, позволяющего автоматизировать процесс сбора и анализа информации, необходимой для выявления уязвимостей.

3. **Третья фаза**. В рамках третьей фазы дается фактическая оценка риска безопасности на основе ущерба, который может быть нанесен организации в случае успешной реализации каждого из сценариев, определенных в профилях атак. Для оценки риска используется качественная шкала с тремя возможными уровнями - низкий, средний и высокий. По результатам анализа рисков разрабатываются рекомендации, направленные на их минимизацию.

**В процессе управления рисками могут предприниматься следующие типы действий**:

* уменьшение риска за счет использования организационных и технических средств защиты, позволяющих снизить вероятность проведения атаки или уменьшить возможный ущерб от атаки;
* уклонение от риска путем изменения архитектуры или схемы информационных потоков автоматизированной системы, что позволяет исключить возможность проведения той или иной атаки;
* изменение характера риска в результате принятия мер по страхованию;
* принятие риска в том случае, если он уменьшен до того уровня, на котором он не представляет опасности для автоматизированной системы.

**Особенности процесса стандартизации в Интернете**

В Глобальной сети уже давно существует целый ряд комитетов, которые занимаются стандартизацией всех интернет-технологий. Эти организации, составляющие основную часть Рабочей группы инженеров Интернета (Internet Engineering Task Force, IETF), уже стандартизировали нескольких важных протоколов, тем самым ускорив их внедрение в сети. Семейство протоколов для передачи данных TCP/IP, SMTP и POP для электронной почты, а так же SNMP (Simple Network Management Protocol) для управления сетью - результаты деятельности IETF.

За несколько последних лет сетевой рынок стал свидетелем так называемого фрагментированного влияния на формирование стандартов. По мере того, как Интернет ширился и обретал черты потребительского и коммерческого рынка, некоторые фирмы стали искать пути влияния на стандартизацию, создав подобие конкурентной борьбы. Давление почувствовали даже неформальные органы, такие как IETF. По мере развития рынков, связанных с Интернетом, предприниматели начали объединяться в специальные группы или консорциумы для продвижения своих собственных стандартов. В качестве примеров можно упомянуть OMG (Object Management Group), VRML (Virtual Reality Markup Language) Forum и Java Development Connection. Порой стандарты де-факто задают своими покупками или заказами серьезные потребители интернет-услуг.

Одна из причин появления различных групп по стандартизации состоит в противоречии между постоянно возрастающими темпами развития технологий и длительным циклом создания стандартов.

**Стандарты безопасности в Интернете**

В качестве средств обеспечения безопасности в сети Интернет популярны протоколы защищенной передачи данных, а именно SSL (TLS), SET, IP v. 6. Они появились сравнительно недавно, и сразу стали стандартами де-факто.

**SSL (TLS)**

Наиболее популярный сейчас сетевой протокол шифрования данных для безопасной передачи по сети представляет собой набор криптографических алгоритмов, методов и правил их применения. Позволяет устанавливать защищенное соединение, производить контроль целостности данных и решать различные сопутствующие задачи.

**SET**

SET (Security Electronics Transaction) - перспективный протокол, обеспечивающий безопасные электронные транзакции в Интернете. Он основан на использовании цифровых сертификатов по стандарту Х.509 и предназначен для организации электронной торговли через сеть.

Данный протокол является стандартом, разработанным компаниями "MasterCard" и "Visa" при участии "IBM", "GlobeSet" и других партнеров. С его помощью покупатели могут приобретать товары через Интернет, используя самый защищенный на сегодняшний день механизм выполнения платежей. SET - это открытый стандартный многосторонний протокол для проведения платежей в Интернете с использованием пластиковых карточек. Он обеспечивает кросс-аутентификацию счета держателя карты, продавца и банка продавца для проверки готовности оплаты, а также целостность и секретность сообщения, шифрование ценных и уязвимых данных. SET можно считать стандартной технологией или системой протоколов выполнения безопасных платежей на основе пластиковых карт через Интернет.

**IPSec**

Спецификация IPSec входит в стандарт IP v. 6 и является дополнительной по отношению к текущей версии протоколов TCP/IP. Она разрабатывается Рабочей группой IP Security IETF. В настоящее время IPSec включает три алгоритмо-независимых базовых спецификации, представляющих соответствующие RFC-стандарты.

Протокол IPSec обеспечивает стандартный способ шифрования трафика на сетевом (третьем) уровне IP и защищает информацию на основе сквозного шифрования: независимо от работающего приложения, шифруется каждый пакет данных, проходящий по каналу. Это позволяет организациям создавать в Интернете виртуальные частные сети. IPSec работает поверх обычных протоколов связи, поддерживая DES, MD5 и ряд других криптографических алгоритмов.

**Обеспечение информационной безопасности на сетевом уровне с помощью IPSec включает:**

* поддержку немодифицированных конечных систем;
* поддержку транспортных протоколов, отличных от ТСР;
* поддержку виртуальных сетей в незащищенных сетях;
* защиту заголовка транспортного уровня от перехвата (предохранение от несанкционированного анализа трафика);
* защиту от атак типа "отказ в обслуживании".

**Кроме того, IPSec имеет два важных преимущества:**

1. его применение не требует изменений в промежуточных устройствах сети;
2. рабочие места и серверы не обязательно должны поддерживать IPSec.