Информационные системы и информационные технологии в государственном управлении.

Технологии, связанные с информационным обеспечением процессов управления, называют новыми информационными технологиями (НИТ), под которыми понимают совокупность современных форм, методов и средств автоматизации информационной деятельности в различных сферах и, в первую очередь, в экономике и организационном управлении. Создаваемые информационная, техническая, программная и технологическая базы информатизации способны обеспечить потребности региона (города) в решении необходимых задач управления.

Административное управление мэрии основывается на широком использовании распространенных общепользовательских и специализированных программных продуктов. Информатизация этого вида деятельности должна обеспечивать:

- работу должностных лиц с нормативно-справочной информацией;
- ведение учета и отчетности технических, материальных, финансовых и других ресурсов;
- осуществление планирования и контроля выполнения планов;
- применение в процессе деятельности должностных лиц расчетных задач и моделирования ситуаций;
- осуществление проектирования и макетирования документации;
- статистическую обработку данных;
- ведение служебной переписки;

оформление нормативно-распорядительной и финансовой документации.

Распределение по функциональным подсистемам определяет основу структуры ИС города, так как информация в них легко структурируется по предметному признаку, обеспечивая необходимую унификацию для автоматизации процессов сбора, обработки, хранения, накопления в банках данных и использования информации в пределах подсистемы. В интересах совместно решаемых задач между подсистемами осуществляется автоматизированный обмен информацией, что обеспечивает функционирование системы в целом. .

Автоматизированная информационная система (АИС) представляет собой совокупность информации, экономико-математических методов и моделей, аппаратно-программных, организационных, технологических средств и специалистов.

По мере развития автоматизированных систем все больше проявляется характер их взаимного влияния и взаимодействия различных сфер информационного обеспечения. В настоящее время преобладает доктрина формирования единой информационной сферы, в которой информацию необходимо классифицировать по разным признакам.

В автоматизированных системах информационное обеспечение делят на *машинное* (в памяти компьютера) и *внемашинное* (на бумажных носителях). Различные классификации предлагались и использовались в системах управления, как правило, для информации, создаваемой и хранящейся в форме документов (приказов, планов, писем, справочно-табличных форм статистической отчетности и т. п.), т.е. в виде *документальной* информации. Однако по мере развития автоматизированных средств появилась возможность регистрации и хранения информации в виде отдельных фактов (характеристик предметов, событий, операций и т. п.), т. е. в виде массивов *фактографической* информации, в которых данные могут сортироваться по различным признакам и выводиться в различных формах, удобных для решения той или иной управленческой или проектной задачи.

Информационная система (ИС) – это система сбора, хранения, накопления, поиска и передачи информации, применяемой в процессе управления или принятия решений.

Экономическая информационная система (ЭИС) представляет собой совокупность внутренних и внешних потоков информации экономического объекта, методов, средств, специалистов, участвующих в процессах сбора, хранения, обработки, поиска и выдачи необходимой информации, предназначенной для выполнения функций управления.

Информационные системы в свою очередь делят на *информационно-справочные*, которые выполняют задачу обеспечения руководства необходимыми справочными данными по запросам, и *информационно-советующие,* в которых кроме сбора, передачи и обработки информации подготавливаются рекомендации, используемые при принятии решений.

Управляющие системы делят на *информационно-управляющие* (например, система управления проектами), *управляющие системы с запрограммированными командами*, в которых решаются задачи регулирования (например, АСУТП), *самонастраивающиеся* и *самообучающиеся* системы, функционирование которых меняется в зависимости от воздействия внешней среды.

По *степени централизации* обработки информации выделяют *системы, имеющие несколько уровней обработки информации* (характерны для крупных объектов), *системы с централизованной обработкой информации* (характерны для средних объектов), *системы коллективного пользования* (характерны для малых объектов).

По *уровню управления* различают системы, относящиеся к *низшему уровню* управления (АСУП – для уровня предприятий и организаций, АСОУ, АСУТП и т.д.), *среднему уровню* управления (ОАСУ – отраслевые АСУ, РАСУ – республиканские и региональные АСУ территориальных органов и др.)

и *высшему уровню* управления (ОГАС – общегосударственная автоматизированная система).

Системы нормативно-методического обеспечения управления предприятием (организацией) как документально-фактографические ИПС. При переходе к правовому государству, а также в процессе развития рыночной экономики возрастает роль еще одного важного вида информации – нормативно-правовой и нормативно-методической, регламентирующей деятельность предприятий при предоставлении им самостоятельности и сокращении организационно-распорядительной документации (стандартов, приказов и распоряжений).

Системы нормативно-методического обеспечения управления (СНМОУ) предприятием регламентируют деятельность подразделений и всех исполнителей управленческих функций. В числе нормативной документации предприятий нормативно-правовые, нормативно-методические, нормативно-технические и организационно-распорядительные документы (НПД, НМД, НТД и ОРД), которые обеспечивают реализацию принятых проектных и управленческих решений при создании и в процессе функционирования предприятия (организации).

Виды систем государственного управления.

Информация является одним из основных элементов социального управления. Информационное обеспечение является базой, на которой строится управленческая деятельность государственного аппарата. Информацию здесь следует рассматривать как некую совокупность различных сообщений, сведений, данных о соответствующих предметах, явлениях, процессах, отношениях и т.д.

Эти сведения будучи собранными, систематизированными и преобразованными в пригодную для использования форму играют в управлении исключительную роль.

Как научная категория информация в управленческих структурах характеризуется рядом признаков (свойств), к числу которых относится известная самостоятельность данных; возможность их многократного использования, сохранения у передающего или получающего субъекта; пригодность к обработке, интеграции и «сжатию» объема за счет изживания

дублирующей, повторной и параллельной информации; допустимость математического анализа; системность, коммуникативность. Говоря о системе государственного управления как о информационной системе, она представляет собой разветвленную сеть линий коммуникаций и баз данных, обеспечивающих циркулирование информации, поступление ее во все структуры, подразделения государственных органов.

Особенно актуально формирование системы содержания информации, нужной для рационального и эффективного государственного управления. В числе единиц такой информации следует выделить:

. сведения, отражающие материальные, производственные, социальные, технические и технологические параметры управляемых объектов;

. данные о нормах, нормативах, стимулах, регулирующих производственную, социально-обслуживающую, духовно-культурную, и иную, имеющую потребительский характер, деятельность управляемых объектов;

. материалы, определяющие деятельность государственных органов в сфере управления (законодательные и иные нормативные правовые акты, договорные обязательства и плановые задания, указания вышестоящих органов, результаты контрольных актов и т.д.);

. сведения о количественном и качественном составе, уровне подготовки

Системы могут быть разделены на документальные, фактографические и документально-фактографические.

Системы гос управления в свою очередь делят на информационно-справочные, которые выполняют задачу обеспечения руководства необходимыми справочными данными по запросам, и информационно-советующие, в которых кроме сбора, передачи и обработки информации подготавливаются рекомендации, используемые при принятии решений.

3. Информационное обеспечение государственного управления.

Основу государственного управления составляет информация, которую мы определим как *совокупность каких-либо сведений, характеристик чего-либо, фактов, данных о соответствующих предметах, явлениях, процессах, отношениях, событиях и т.д., собранных и систематизированных в пригодную для использования форму.*

Информационное обеспечение государственного управления – *это система концепций, методов и средств, предназначенных для обеспечения пользователей (потребителей) информацией.*

Система информационного обеспечения – *включает в себя информационные ресурсы, организационно-функциональное, функциональное, программное, техническое, технологическое,правовое, кадровое и финансовое обеспечение и предназначена для сбора, обработки, хранения и выдачи информации пользователям.*

Информационный ресурс - *это сведения (данные), организованные в системах информационного обеспечения в виде фондов на физических носителях (базах данных, библиотеках, архивах), находящиеся в собственности или распоряжении и пользовании юридических или физических лиц.*

Управленческая информация - *часть социальной информации, которая выделена из общего массива по критериям пригодности к обслуживанию государственно-правовых процессов формирования и реализации управляющих воздействий*.

Выделяют следующие источники, объективно порождающие управленческую информацию:

а) *нормы законодательных и иных актов*, управомочивающие госорганы и госслужащих на выполнение каких-то действий в обозначенном времени и направлении;

б) *обращения граждан* в госорганы по реализации своих законных интересов субъективных прав;

в) *обязательные указания* вышестоящих органов, подлежащие выполнению нижестоящими;

г) *факты, отношения*, выявляемые в процессах контроля, различных проверок;

д) *проблемные, конфликтные, экстремальные и иные сложные ситуации,* нуждающиеся в оперативном и активном сильном вмешательстве госорганов и должностных лиц. Такие кризисные ситуации требуют выработку заранее соответствующих алгоритмов управленческих действий. Хотя такие ситуации неповторимы, все равно по каждой из них должны быть продуманы и

отрепетированы модели быстрого и энергичного вмешательства конкретных госструктур и должностных лиц.

Управленческая информация должна соответствовать требованиям актуальности, достоверности, достаточности, доступности и аутентичности (выражение в понятной людям форме).

Нынешний этап информатизации государственного управления характеризуется резким возрастанием информационных потоков и созданием таких информационных средств и технологий, которые в корне изменили все информационные процессы и интеллектуальное представление о них. Поэтому к сегодняшнему дню все ведущие страны уже определили свою политику и стратегию движения к информационному обществу. Администрация США в 1993 г. утвердила план своих действий в области Национальной информационной структуры. В июле 1994 г. Комиссией Европейского сообщества принят план действий «Европейский путь в информационное общество». Россия также вступила на путь построения информационного общества. Грандиозные по масштабам задачи намечены в Федеральной целевой программе «Электронная Россия».

4. Концепция электронного правительства.

Концепция формирования в Российской Федерации электронного правительства до 2010 года (далее – Концепция) разработана Министерством информационных технологий и связи Российской Федерации совместно с Министерством экономического развития и торговли Российской Федерации и Федеральной службой охраны Российской Федерации.

Под электронным правительством в Концепции понимается новая форма организации деятельности органов государственной власти, обеспечивающая за счет широкого применения информационно-коммуникационных технологий качественно новый уровень оперативности и удобства получения организациями и гражданами государственных услуг и информации о результатах деятельности государственных органов.

Концепция основывается на Концепции использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года, одобренной распоряжением Правительства Российской Федерации от 27 сентября 2004 года №1244-р, а также на Концепции административной реформы в Российской Федерации в 2006-2010 годах, одобренной распоряжением Правительства Российской Федерации от 25 октября 2005 года №1789-р.

Концепция определяет основные приоритеты, направления и этапы формирования в Российской Федерации электронного правительства на период до 2010 года.

В соответствии с Концепцией разработан план мероприятий по ее реализации.

Электронное правительство один из элементов информационного общества. Использование современных информационно-телекоммуникационных технологий в организации государственного менеджмента обеспечит новое качество услуг гражданам и бизнесу со стороны государственных служб. Сам государственный аппарат должен превратиться в бизнес – эффективный бизнес, оправдывающий затраты на себя со стороны налогоплательщиков и максимальное уменьшение расходов на свою деятельность. Автоматизированные государственные службы обеспечат свободный доступ граждан ко всей необходимой государственной информации, обеспечат сбор налогов,

регистрацию транспортных средств и патентов, заключение различных соглашений и т.д. Это может привести также к открытости и прозрачности деятельности органов управления.

В западном восприятии электронное правительство состоит из трех основных модулей:

- G2G (government to government, правительство правительству);
- G2B (government to business, правительство бизнесу);
- G2C (government to citizens, правительство гражданам).

Электронное правительство включает:

- *он-лайновые сервисы* для праждан и бизнесов на едином портале;
- *электронный документооборот* в правительственных и парламентских структурах,
- *общую* для разных правительственных структур *базу данных* для предотвращения дублирования информации и повторных затрат;
- часто – закрытую специализированную информационную сеть (*интранет*) для внутриправительственных транзакций;
- разветвленную *информационно-телекоммуникационную инфраструктуру*;
- системы *криптографии* и прочие способы защиты *информации* в том числе и персональных данных;
- *цифровую подпись*;
- *электронный ключ*;
- *смарт-карты*;
- другие средства санкционированного доступа к информации и операций с ней.

Электронное правительство тесно связано с такими компонентами информационного общества как *электронная коммерция, электронный бизнес, электронный банкинг, универсальный доступ, пожизненное образование, компьютеризация, компьютерная грамотность*.

G2G-модуль электронного правительства.

Итак, в целом функции сервиса “правительство правительству” можно охарактеризовать как удешевление работы правительства, ускорение прохождения документов через его структуры, увеличение возможностей контроля за деятельностью отдельных органов и служащих, увеличение конкуренции между служащими и повышение их квалификации, и главное – предотвращение коррупции.

Анализируя возможности и функции электронного правительства как новой модели государственного управления, особое внимание следует уделить следующей его характеристике. Электронное правительство трансформирует не только отношения граждан и властных структур, но и отношения внутри правительства – между отдельными его ветвями, уровнями, подразделениями. Причем изменению подвергается не, только сетевая инфраструктура исполнительной власти, но в целом вся инфраструктура государственной власти и управления. То есть, с этой точки зрения электронное правительство точнее будет назвать электронным государством, электронным государственным аппаратом, электронной инфраструктурой государства, государством Информационного общества.

Говоря об электронном правительстве и в частности о внедрении сектора G2G, следует понимать, что прежде всего речь идет об информатизации всех управленческих процессов в органах государственной власти всех уровней, об информатизации межведомственных взаимоотношений, о создании компьютерных систем, способных поддерживать все функции взаимодействия этих органов с населением и бизнес-структурами. Итак, кроме использования ИТ и создания информационных ресурсов, электронное правительство требует принятия соответствующей нормативно-правовой базы. Так, следует законодательно закрепить норму, согласно которой электронный документ не является просто электронной копией бумажного, а что это первичный, т.е. главный документ, с которым можно работать так же в электронном виде. Это означает, в свою очередь, потребность в законе об электронной цифровой подписи, об электронном документообороте, о защите данных, об обучении и аттестации служащих, о формах сотрудничества правительственных структур с ИТ-компаниями и т.д.

Основа гражданского общества – правительственные сервисы для граждан и бизнесов

Этот раздел мы посвятим изучению еще двух аспектов электронного правительства как социального явления, а именно – работе модулей G2B и G2C. Основные же задачи сервисов “правительство-гражданину” и “правительство-бизнесу” (формулы G2C и G2B) в рамках реализации проекта электронного правительства можно определить следующим образом: преодоление бюрократии, внедрение в правительственных структурах ориентированности на граждан, высвобождение ресурсов, избавление от очередей, упрощение легализации частной инициативы в сфере бизнеса, активизация малого и среднего бизнеса в стране, оптимизация государственного менеджмента, удешевление ведения бизнеса путем внедрения телеработы и оцифровывания документооборота.

Итак, правительственный ресурс должны характеризовать: информативность; наличие внутренней поисковой машины; функциональность; дружественность интерфейса; наличие он-лайнового сервиса; наличие почты; уровень дизайна; наличие функций для обслуживания пользователей с физическими ограничениями; наличие интернет-адресов других государственных служб; наличие текстов принятых документов; наличие справочных и вспомогательных ресурсов для заполнения форм, оформления заявок и т.д.; наличие портрета главы структуры;

Электронное правительство и цифровая демократия

Кроме оптимизации механизмов государственного управления за счет постепенного внедрения функциональных модулей G2G, G2B и G2C, электронное правительство активизирует такой социально значимый процесс как формирование цифровой (электронной) демократии. Пожизненное обучение, телематика, компьютеризация, компьютерная грамотность, универсальный доступ, активное правление, электронная почта, электронное голосование, электронное правительство, интернет и прочие элементы информационного общества, внедрению которых прямо или опосредствованно оказывает содействие создание электронного правительства, активизируют социальную

позицию граждан, подталкивают их к более широкому использованию своих прав и свобод.
Демократия, обогащенная возможностями ИТ и включенная в общую систему ценностей информационного общества, является важным достижением государства и гражданина, причем это касается многих вещей. Традиционные способы ее осуществления имеют много недостатков, хотя демократия и остается по сей день наилучшей формой правления.

5. Организации РФ, осуществляющие контрольные и нормативно-методического характера функции по отношению ко всем государственным информационным ресурсам.

Этим занимаются ☺ вот они:

* Министерство Российской Федерации по связи и информатизации – контроль за созданием информационных ресурсов в органах и организациях, их регистрацией, доступностью и порядком использования, а также контроль систем навигации и общая координация работ по формированию и ведению государственных информационных ресурсов.

* Федеральное агентство правительственной связи и информации при Президенте РФ и Государственная техническая комиссия при Президенте РФ – контроль за защитой государственных информационных ресурсов от незаконного использования и разрушения.

* Министерство имущественных отношений РФ – учет государственных информационных ресурсов как имущества, порядка их закрепления в оперативном управлении и хозяйственном ведении.

* Российское агентство по патентам и товарным знакам – учет информационных ресурсов как интеллектуальной собственности.

Министерство финансов РФ – порядок финансирования и финансовой отчетности деятельности по формированию информационных ресурсов с использованием бюджетных средств, а также оказания платных услуг на основе государственных ресурсов.

В 1999 г. Межведомственной группой специалистов под руководством Минсвязи России, подготовлен доклад «Информационные ресурсы России», в котором подробно рассмотрены состояние, тенденции развития государственных информационных ресурсов и выделены основные категории информационных ресурсов России.

6. Государственные информационные ресурсы России:

1) Информационные ресурсы библиотечной сети России

Не смотря на недостаточные объемы финансирования библиотечная сеть России продолжает функционировать и насчитывает около 150 тыс. библиотек. Только в 2,5 тыс. научных и публичных библиотек используются автоматизированные библиотечно-информационные технологии. Наиболее значительные базы данных сформированы в библиотек ИНИОН, Российской

национальной библиотеке, Российской государственной библиотеке, Государственной публичной научно-технической библиотеке России.

Под эгидой Минкультуры РФ реализуется программа «Создание общероссийскойинформационн-библиотечной компьютерной сети – ЛИБНЕТ».

Сайт www. gpntb.ru ГПНТБ

2) Ресурсы государственной системы экономической и научно-технической информации.

Одним из важных элементов ГСНТИ является объединение Росинформресурс Минпромнауки России (www.rosinf.ru). Здесь можно получить информацию:

- о новых технических решения в промышленности, строительстве, с/х, торговле и т.т.д.
- о рынке промышленной продукции (о продукции, товарах и услугах 57 тыс. предприятий)

3) Российские ресурсы правовой информации.

Государственные и коммерческие системы.

Коммерческие организации – разработчики правовых систем достаточно полно представлены в Интернет:

- НПП «Гарант-сервис» - www.garant.ru;
- Консорциум «Кодекс» - www.kodeks.net;
- АО «Консультант Плюс» - www.consultant.ru.

4) Информационные ресурсы федеральных и региональных органов власти.

- информация о земельных ресурсах;
- информация об объектах недвижимости;
- информация о юридических лицах;
-информация о физических лицах;
- нормативно-правовые документы;
- социально-экономические и финансовые показатели административно-территориальных единиц и хозяйствующих объектов.

www.lenobl.ru

5) Информационные ресурсы в сфере финансов и внешнеэкономической деятельности.

www.minfin.ru

www.cbr.ru

www.gtk.ru

6) Информационные ресурсы отраслей материального производства.

Основу информационных ресурсов предприятий и организаций отраслей материального производства составляют документы и электронные массивы информации, созданные и используемые в процессе их деятельности.

www.vpk.ru. Общая информация о деятельности ВПК, справочная информация о крупных предприятиях ВПК, сводная информация о товарах и услугах предприятий и организаций ВПК.

7) Информационные ресурсы Государственной системы статистики.

Сайт Госкомстата www.gks.ru. С него переход на сайты:

- *Информационный центр Госкомстата России*;

- *Главный межрегиональный центр обработки и распространения информации Госкомстата России (ГМЦ).*

В состав информационного фонда ГМЦ входят сведения :

- *о промышленности,*
- *сельское хозяйство,*
- *наука и инновации,*
- *уровень жизни и доходы населения,*
- *статистика внешнеэкономической деятельности,*
- *паспорт территории РФ,*
- *регистр городов России,*
- *единый государственный реестр предприятий и организаций России (ЕГРПО)* Сведения о 2 700 000 юридических лиц,
- *бухгалтерская отчетность,*
- *регистр промышленных предприятий,*
- *регистр сельскохозяйственных предприятий.*

Доступ к подавляющей части статистических публикаций является платным.

8) Информационные ресурсы социальной сферы.

В состав наиболее значимых отраслей социальной сферы входят:

- *здравоохранение;*
- *образование;*
- *занятость и социальное обеспечение;*
- *пенсионное обеспечение;*
- *миграционная служба;*
- *физическая культура и туризм.*

Наиболее важные информационные услуги в социальной сфере:

- наличие лекарств в оптовой и розничной торговле (www.pharm.mos.ru для Москвы);
- сведения о путевках в санатории и в путешествия и т.д.

9) Информация о природных ресурсах, явлениях, процессах.

Информация о природных ресурсах, явлениях и процессах сосредоточена в нескольких отраслевых системах и секторах информационной сферы. Наиболее крупной из этих систем является создаваемая в Министерстве природных ресурсов РФ *Единая информационная система недропользования (ЕИСН)*. В ее состав входят:

Всероссийские геологические фонды – Росгеофонд 5 специализированных и 62 территориальных геофондов субъектов РФ;

Государственный банк цифровой геологической информации (ГБЦГИ);

Банк данных государственного мониторинга геологической среды (ГМГС);

Музейно-библиотечные и коллекционные фонды, фонды эталоновминерального сырья и кернового материала.

В этих фондах сосредоточено много ценной научной информации. Например, представлены результаты наблюдений за гидрометео обстановкой с 1725 года. Ознакомиться с геоинформационными сведениями можно на сайтах: www.gbdgi.ru, www.gisa.ru, www.fccland.ru

7. Основные этапы создания компьютерных систем.

Создание информационных систем и информационных технологий представляет собой сложный процесс. К настоящему времени определились основные этапы их построения:

- *принятие решения* о создании информационной системы с определением ответственного лица за эту работу. Очень важно, чтобы таким лицом было первое лицо предприятия. Для нашей страны важным является первое директивное указание о начале проведения таких работ - Постановление ЦК КПСС и Совета Министров СССР от 6 марта 1966 г. «Об улучшении организации работы по созданию и внедрению в народное хозяйство средств вычислительной техники и автоматизированных систем управления»;
- *проведение предпроектного исследования* объекта управления. В процессе предпроектного исследования выявляются наиболее существенные характеристики объекта, изучаются его внешние и внутренние информационные потоки, создаются математические и физические модели исследуемой системы и ее элементов, устанавливаются условия взаимодействия человека и технических средств управления. Значительное внимание уделяется детальной разработке архитектуры информационной системы в целом, а также проектных решений по отдельным ее объектам и элементам, их анализу, практической апробации и внедрению. Заканчивается этот этап разработкой технического задания;
- *разработка технического проекта*, в котором решаются все принципиальные вопросы построения системы;
- *рабочее проектирование* (разработка программ, словарей, установка технических средств, эксплуатационной документации и т.д.;
- *организация приемо-сдаточных* испытаний для внедрение информационной системы в опытную эксплуатацию;
- *промышленная эксплуатация информационной системы.*

8. Система централизованной обработки данных

Современное производство требует высоких скоростей обработки информации, удобных форм ее хранения и передачи. Необходимо также иметь динамичные способы обращения к информации, способы поиска данных в заданные временные интервалы; реализовывать сложную математическую и логическую обработки данных. Управление крупными предприятиями, управление экономикой на уровне страны требуют участия в этом процессе достаточно крупных коллективов. Такие коллективы могут располагаться в разных районах города, в различных регионах страны и даже в различных странах. Для решения задач управления, обеспечивающих реализацию экономической стратегии, становятся важными и актуальными скорость и удобство обмена информацией, а также возможность тесного взаимодействия всех участвующих в процессе выработки управленческих решений.

На первом этапе становления информационных систем и информационных технологий использовалась централизованная обработка данных.

В эпоху централизованного использования ЭВМ с пакетной обработкой информации пользователи вычислительной техники предпочитали приобретать компьютеры, на которых можно было бы решать почти все классы их задач. Однако сложность решаемых задач обратно пропорциональна их количеству, и это приводило к неэффективному использованию вычислительной мощности ЭВМ при значительных материальных затратах. Нельзя не учитывать и тот факт, что доступ к ресурсам компьютеров был затруднен из-за существующей политики централизации вычислительных средств в одном месте.

9.Система распределенной обработки данных

Появление малых, микро ЭВМ и ПК потребовало нового подхода к организации систем обработки данных, к созданию новых информационных технологий. Возникло обоснованное требование перехода от использования централизованной обработки данных к распределенной обработке данных.

Распределенная обработка данных- это обработка данных, которая выполняется на независимых, но связанных между собой компьютерах, представляющих распределенную систему. Выглядит распределенная система так:

Для реализации распределенной обработки данных были созданы многомашинные ассоциации (- это совокупность вычислительных машин различной производительности, объединенных в систему с помощью каналов связи)

10.Компьютерные (вычислительные) сети

- это совокупность компьютеров и терминалов, соединенных с помощью каналов связи в единую систему, удовлетворяющих требованиям распределенной обработки данных.

Основное назначение компьютерной сети - предоставление информационных и вычислительных ресурсов пользователям.

Вычислительные сети можно разделить на 3 класса в зависимости от расположения абонентских сетей (Абонентские сети - это элементы, потребляющие информацию в сети):

- Глобальные
- Региональные
- Локальные

Глобальные, региональные и локальные вычислительные сети создают иерархию компьютерных сетей.

Схема структура вычислительной сети:

11. Глобальные вычислительные сети. Интернет.

В ГВС используется принцип коммутации не каналов (как у их прародительницы – телефонных сетей), а пакетов, когда данные разделяются на небольшие порции – пакеты, - которые самостоятельно перемещаются по сети за счет встраивания адреса конечного узла в заголовок пакета.

Примером глобальной вычислительной сети является Интернет (всемирная сеть), появившийся в начале 90-х гг. Период его становления занял где-то 20 лет. Его предшественником была военная сеть Министерства обороны США ARPANet, начавшая функционировать в начале 70-х гг.

Интернет (*interconnected networks*) – динамично развивающая структура, не принадлежащая никакому частному лицу или фирме. Ее использованием и дальнейшим развитием занимаются тысячи различных организаций. Тем не менее в Интернет поддерживается определенный порядок, и сеть развивается в соответствии с определенными правилами.

Ассоциация за Прогрессивные Телекоммуникации
(Association for Progressive Communications (APC)), Российский институт общественных связей (**ripni.ru)**

Услуги Интернет:

- *электронная почта* (e-mail);
- *участие в телеконференциях* (Usenet);
- *доступ к базам данных* FTP, Gopher, WWW.

1. У Интернета нет собственника, так как он является совокупностью сетей, которые имеют различную географическую принадлежность.
2. Интернет нельзя выключить целиком, поскольку маршрутизаторы сетей не имеют единого внешнего управления.
3. Интернет может связать каждый компьютер с любым другим, подключённым к Сети, так же, как и телефонная сеть. Если телефон имеет автоответчик, он способен распространять информацию, записанную в него, любому позвонившему.

К середине 2008 года число пользователей, регулярно использующих Интернет, составило около 1,5 млрд человек (около четверти населения Земли).

Всемирная компьютерная сеть Интернет вместе с персональными компьютерами образует технологическую основу для развития международной концепции «Всемирного информационного общества».

В России почти все средние школы с 2008 года оснащены компьютерами с доступом к сети Интернет и базовыми пакетами программ для обучения информатике, работе с персональными компьютерами и сетью Интернет

2. Основные термины.

bps (bits per second) - бит в сек (бод), единица скорости передачи данных.

Browser - (браузер) программа просмотра документов в Интернет: либо **Internet Explorer**, либо **Net Scape.**

DNS (Domain Name System) - доменная система адресации с преобразованием имени компьютера в числовой адрес Интернет.

Domain - праввая часть электронного адреса.
FAQ (Frequently Asked Questions) - часто спрашиваемые вопросы.
FTP (File Transfer Protocol) - протокол передачи файлов.
HTML (Hyper Text Markup Language) - язык разметки гипертекстовых файлов в системе WWW.
Login - левая часть электронного адреса.
Protocol - метод, используемый для передачи сообщения от хоста к вашему компьютеру
Rambler - русскоязычная поисковая система в Интернет
TCP/IP - форма передачи сообщений в Интернет
URL (Uniform Resource Location) - уникальный адрес документа в интернет.
WWW (World Wide Web) - «всемирная паутина». Гипертекстовая система поиска ресурсов Интернет.
Провайдер - организация, предоставляющая доступ в Интернет
Сервер (хост-компьютер) - компьютер с материалами информационного, коммерческого или рекламного характера. Обычно свободный доступ.

2. Поиск информации в Интернет

2.1. Желтые страницы Интернет

- Книги (мировые и российские ресурсы);
- CD-ROM
-http//www.piter-press/ru/koi/yp/full_version/yp-start.htm;

2.2. Индексные системы глобального поиска:

Alta Vista (hw.altavista.com) всемирные индексы;
Rambler (hw.rambler.ru) российские индексы;
Yandex (hw.yandex.ru) отечественный индексы;
АПОРТ! **(**hw.aport.ru) русскоязычная система.

2.3. Систематические каталоги

Yahoo! (hw.yahoo.com) патриарх каталогов Интернет
«**АУ!»** (http://russia.agama.com/ru) каталог России;
«Созвездие» (hw.stars.ru) каталог России.

2.4.Специализированные каталоги:

SEARCH.COM (hw.search.com)
HotBot (hw.hotbot/index.html) - поиск не серверов,
Switchboard (hw.switchboard.com/) а людей.
Mining Company **(**hw.mining.com) ручная подборка материалов

12. Программное и техническое обеспечение компьютерных сетей.

Общими компонентами всех сетей являются:

- Серверы (server) – компьютеры, предоставляющие свои ресурсы сетевым пользователям;
- Клиенты (client), – компьютеры, осуществляющие доступ к сетевым ресурсам, предоставляемыми сервером;
- Среда (media) – средства передачи информации;
- Совместно используемые данные – файлы, передаваемые серверами по сети;
- Совместно используемые периферийные устройства.

Виды технического обеспечения компьютерных сетей:

- **Кабели. (*Коаксиальный кабель, Ethernet-кабель*)**
- **Адаптеры.** Вне зависимости от используемого кабеля для каждой рабочей станции необходимо иметь сетевой адаптер. Сетевой адаптер – это плата, которая вставляется в материнскую плату компьютера. Она имеет два разъема для подключения к сетевому кабелю.
- **Репитер.** Если длина сети превышает максимальную длину сегмента сети, необходимо разбить сеть на несколько (до пяти) сегментов, соединив их через репитер.
- **Серверы.** Для обеспечения функционирования локальной сети часто выделяется специальный компьютер – сервер, или несколько таких компьютеров. На дисках серверов располагаются совместно используемые программы, базы данных и т.д. Остальные компьютеры локальной сети часто называются рабочими станциями. В сетях, состоящих более чем из 20-25 компьютеров, наличие сервера обязательно – иначе, как правило, производительность сети будет неудовлетворительной.
- **Модемы и факс-модемы.** Модемы - это устройство для обмена информацией с другими компьютерами через телефонные сети. Факс-модем – устройство, сочетающее возможности модема и средства для обмена факсимильными изображениями с другими факс-модемами и обычными телефаксными аппаратами.
- **Оборудование для беспроводной связи. *Радиомодемы,*** выпускаемые сегодня многими фирмами, соединяют между собой компьютеры в помещеньях, где по какой-то причине нельзя прокладывать кабели и сверлить стены. Ц***ифровая сотовая связь*** для портативных компьютеров.

Международный информационный обмен — передача и получение информационных продуктов, а также оказание информационных услуг через государственную границу.

Программное обеспечение (ПО) – совокупность программ, позволяющая организовать решение задачи на компьютере.

Важнейшими классами ПО являются системное и функциональное (прикладное).

Планировщик	Автоматизация управленческой деятельности организации
Супервизор	Автоматизация малого бизнеса
Сервисные обслуживающие	Формирование бизнес-плана
Редактор связей	Финансовый анализ
Отладчик	Правовые Базы данных
Утилиты	Автоматизация банковской деятельности
	Обучающие программы

13. Требования, предъявляемые к комплексу технических средств информационных систем.

Информационная система управления – совокупность информации, экономико-математических методов и моделей, технических, программных, других технологических средств и специалистов, предназначенная для обработки информации и принятия управленческих решений, а также для снабжения необходимой информацией граждан и бизнес-организаций. Имеется в виду вопросы регистрации малого бизнеса, представления им налоговых льгот и т.д.
Для эффективной работы ИнфоСист – **ряд требований**. КТС – комплекс технич.сред-в (главный элемент КТС – ЭВМ или комп).

- минимизация трудовых и стоимостных затрат на решение всего комплекса задач системы;
- реализация интегрированной обработки информации за счет информационной, технической и программной совместимости различных технических устройств;
- обеспечение пользователей связью через терминальные устройства с распределенной базой данных;
- высокая надежность;
- наличие защиты информации от несанкционированного доступа;
- реализуемость КТС, т.е. возможность его создания за счет типовых средств, выпускаемых отечественной промышленностью;
- гибкость структуры КТС, т.е. перспектива включения в нго состав новых, более совершенных технических средств по мере освоения их промышленностью.
- Главным элементом КТС, конечно, является ЭВМ или компьютер.
- Характерными чертами современных компьютеров являются:
- высокая производительность;

- разнообразие форм обрабатываемых данных – двоичных, десятичных, символьных, при большом диапазоне их изменения и высокой точности представления;
- обширная номенклатура выполняемых операций, как арифметических, логических, а также специальных;
- большая емкость оперативной памяти;
- развитая организация системы ввода-вывода информации, обеспечивающая подключение разнообразных видов внешних устройств.

14. Автоматизированное рабочее место (АРМ) и его программное обеспечение.

АРМ – одна из форм ИС в управлении предприятиями наряду с индивидуальным использованием компьютеров и локальными вычислительными сетями (ЛВС).
Главное назначение общего ПО – запуск прикладных программ и управление процессом их выполнения.

Специальное программное обеспечение АРМ состоит из уникальных программ и функциональных пакетов прикладных программ. Именно от функционального ПО зависит конкретная специализация АРМ.

Специальное ПО создается обычно на основе инструментальных программных средств.

Инструментальные программные средства – это программы, ориентированные на решение не одной задачи, а на решение задач со схожими особенностями обработки информации. Пользование ими освобождает пользователя от программирования своей задачи на каком-либо алгоритмическом языке. Для решения своей конкретной задачи пользователь каждый раз как бы настраивает ее на свою задачу.

Классическим примером инструментальных систем являются программы ППП MicroSoft Office:
- MS Word;
- MS Excel;
- MS Access;

Сам ППП MicroSoft Office является классическим примером *интегральных пакетов программ*. В рамках интегрированного пакета обеспечивается одинаковая структура данных в каждой программе, что позволяет обмениваться данными и формировать интегрированные документы. Например, в текст подготовленный программой MS Word, можно вставлять табличные данные или диаграммы, подготовленные программой MS Excel.

15. Стратегия парламентской деятельности.

Эффективная деятельность парламента обеспечивается многими составляющими факторами, прежде всего такими, которые определяют стратегию парламентской деятельности. Под этим понимается система, включающая в себя научно обоснованную концепцию, методологию и средства долгосрочного и

оперативного обеспечения деятельности парламента. Эта деятельность должна ориентироваться на стратегические цели развития общества в целом, его народно-хозяйственных комплексов, отраслей, подотраслей, регионов и других объектов организационного управления, взаимодействия с государствами внешнего мира. Естественно, при этом должны учитываться также проблемы, находящиеся в ведении представительного и законодательного органа (парламента), и компетенция депутатов. От организации работы парламента во многом зависит эффективность разрабатываемых им законов, других нормативных правовых актов.

Деятельность значительного количества специалистов, вовлеченных в законотворчество, обеспечение преемственности опыта депутатских корпусов разных созывов настоятельно требуют систематизации и эффективной организации их повседневной работы на единой концептуальной и методологической основе. К сожалению, в отечественной и зарубежной литературе проблемам обоснования стратегии деятельности парламентов уделяется крайне незначительное внимание.

В укрупненном виде процесс формирования стратегии парламентской деятельности должен включать следующие основные этапы.

1. Анализ целей развития государства на перспективу, на основе которого может быть сформирована база данных (знаний), содержащая "желаемые" состояния государства и его объектов организационного управления. При этом следует использовать результаты прогнозирования развития государства на долгосрочную, среднесрочную и краткосрочную перспективы. Эта работа должна носить не разовый характер, а проводиться на постоянной основе с систематической актуализацией перечня целей.

2. Формирование и анализ перечня актуальных проблем, которые необходимо решать для достижения поставленных государством целей. Те из проблем, что находятся в ведении парламента, должны быть представлены в виде базы данных (знаний), содержащей паспорта проблем, этот перечень также подлежит систематической актуализации.

3. Ранжирование проблем по очередности разработки парламентом соответствующих законопроектов. Это должно обеспечить формирование нормативных правовых актов в виде логически взаимоувязанного и синхронизированного во времени законотворческого процесса.

4. Формирование долгосрочных и оперативных планов (программ) законопроектной работы парламента и создание соответствующих баз данных.

5. Разработка системной технологии законопроектной работы. При этом проекты законов должны "конструироваться" как изделия, проходящие унифицированный жизненный цикл процессов и процедур, начиная от идейного замысла закона (законодательной инициативы) до выпуска "готового продукта" — закона. Учитывая, что в парламенте, как правило, параллельно разрабатываются десятки и сотни законопроектов, фактор организации эффективной совместной деятельности парламентариев и других органов власти и управления приобретает самостоятельное значение. Здесь необходима единая информационно-аналитическая многофазная технология и автоматизированные средства реализации законопроектной работы.

6. Контроль качества разрабатываемых законопроектов на всех стадиях их прохождения, в том числе и по результатам применения законов в реальной жизни (по конечному эффекту).

16. Информационное обеспечение Совета Федерации РФ.

Отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации при применении информационных технологий и обеспечении защиты информации, регулирует Федеральный закон от 27 июля 2006 года№149/ФЗ "Об информации, информационных технологиях и о защите информации" (далее—Закон об информационных технологиях). Закон об информационных технологиях принят как новая редакция Федерального закона от 20 февраля 1995 года№24/ФЗ "Об ин формации, информатизации и защите информации", что представляет определенную сложность. Соответственно, признаны утратившими силу Закон об информатизации и Федеральный закон от 4 июля 1996 года № 85/ФЗ "Об участии в международном информационном обмене".

Работы по информатизации Совета Федерации начались с "чистого листа", при полном отсутствии "начального" функционального, информационного, программного, технического и финансового обеспечения. Многие вопросы, решались благодаря сохранившимся личным и профессиональным контактам.

Стратегия и методология информатизации Совета Федерации определяется указом Президента РФ № 159 от 17 февраля 1995 г. "*О создании Информационно-коммуникационной системы Совета Федерации Федерального Собрания*".

В основе:

а) **модели информационных агрегатов**, отображающие на концептуальном уровне государство, парламент, организационно-функциональную структуру государственно-правовой сферы;

б) результаты фактографического обследования и выявления информационных потребностей составляющих Совета Федерации;

в) **системный анализ информационного взаимодействия** Совета Федерации с участниками государственно-правовой системы (Гос Дума, Президент РФ, Администрация Президента РФ, Правительство РФ, его Аппарат, фед органы РФ, субъекты РФ, их органы, министерства, ведомства РФ, Российская академия наук, государства СНГ, их органы, зарубежные государства, международные организации и др.);

г) **опыт работ по информационному обеспечению других высших гос органов и структур** (Совета Министров СССР, Верховного Совета СССР, Верховного Совета РСФСР, Администрации Президента РФ), и др.

д) организационно-распорядительные документы и системы, обеспечивающие формирование информационного пространства государств - - участников СНГ и автоматизированный обмен информацией между ними;

е) **анализ информатизации парламентской деятельности зарубежных государств**

Информатизация Совета Федерации ведется в следующих разрезах: организационно-функциональном; функциональном; информационном; программном; техническом; технологическом; организационно-кадровом.

Внедрение и развитие информационного обеспечения осуществляется по следующим основным направлениям:

- фактографическое **обследование и анализ информационных потребностей** пользователей Информационно-коммуникационной системы;

- разработка и **внедрение прикладных функциональных задач, формирование информационных ресурсов, баз данных** и поддержание их в актуальном состоянии;

- Создание Информационно-коммуникационной системы (ИКС) Совета Федерации;

- оперативное информационно-справочное обслуживание Совета Федерации и его составляющих;

- организация сети внешних источников информационной поддержки;

- оснащение программно-техническими средствами зданий Совета Федерации;

- обучение служащих Совета Федерации;

- обеспечение информационного взаимодействия Совета Федерации с Гос Думой, Администрацией Президента РФ, Аппаратом Правительства РФ, министерствами, ведомствами, субъектами РФ, Российской академией наук, парламентами стран СНГ и других зарубежных государств.

Информационное обеспечение деятельности Совета Федерации осуществляется на основании информационно-коммуникационной системы Совета Федерации, созданной в соответствии с Указом Президента Российской Федерации от 17 февраля 1995 года № 159 "О создании информационно/коммуникационной системы Совета Федерации Федерального Собрания Российской Федерации". В дальнейшем наращивание информационных технологий и информационных систем осуществлялось на основании Концепции развития информационно-коммуникационной системы Совета Федерации Федерального Собрания

Российской Федерации до 2010 года, утвержденной Руководителем Аппарата Совета Федерации 9 февраля 2006 года и одобренной Комиссией Совета Федерации по контролю за обеспечением деятельности Совета Федерации (протокол № 2 от 6 февраля 2006 года). **Реализация концепции позволила Совету Федерации достичь конкретных результатов в информационном обеспечении законодательной деятельности**, особенно с учетом перехода страны на трехгодичное бюджетное планирование. В рамках Концепции развития информационно-коммуникационной системы Совета Федерации осуществлено внедрение:

- **официального Интернет-сайта** и корпоративного Интранет-сайта Совета Федерации;

- специализированной информационной системы "Парламентский портал" в сети Интернет;

- подсистемы **автоматизированного документооборота** и делопроизводства Совета Федерации "Дело/ТСФ";

- подсистемы "Электронный архив Совета Федерации" с входящим в ее состав "Виртуальным читальным залом";

- подсистемы "**Поточное (пакетное) сканирование документов**"; подсистемы "Автоматизированная web/публикация электронных файлов";

- автоматизированной информационной системы "Материальные и инженерные ресурсы Совета Федерации";

- автоматизированной **информационной системы "Кадры Совета Федерации";**

- **Удостоверяющего центра Совета Федерации, обеспечивающего применение электронной цифровой подписи** в автоматизированных системах информационно/коммуникационной системы Совета Федерации;

- единого комплекса обработки служебной информации в составе информационно/коммуникационной системы Совета Федерации на базе технологии терминального доступа;

- системы электронного документооборота в Совете Федерации Федерального Собрания Российской Федерации;

- технологической системы сбора и публикации информации о членах Совета Федерации и руководителях субъектов Российской Федерации;

- информационной системы "Мониторинг материалов о деятельности Председателя Совета Федерации";

- **информационной системы "Обзор СМИ**";

- информационной системы "Модельные законодательные акты МПА СНГ и МПА ЕврАзЭС";

- информационной системы "Комплекс электронных словарей";

- информационной системы "Электронная версия сборника нормативных правовых актов по вопросам государственной службы и кадровой политики";

- автоматизированной информационно/аналитической системы "Налоговая отчетность", обеспечивающей доступ пользователей к данным налоговой отчетности,

- составление на их основе аналитических справок (отчетов) по поступлению налогов и сборов в зависимости от уровня бюджетов, интервала времени, видов налогов и сборов и прогнозированию поступления налогов и сборов в бюджет;

- автоматизированной информационно/поисковой системы "Совет Федерации: правовые акты";

- автоматизированной информационной системы "Web/представление тезауруса Парламентской библиотеки";

- **автоматизированной информационной системы "Оценка и прогнозирование ситуаций на основе СМИ**";

- автоматизированной информационной системы "Календарь мероприятий Совета Федерации";

- **автоматизированной системы дистанционного обучения работе с информационными системами**;

- **удаленных электронных офисов членов Совета Федерации и работников Аппарата Совета Федерации,** обеспечивающих удаленный беспроводной доступ к внутренним информационным ресурсам Совета Федерации и внешним информационным ресурсам;

- **системы многоканальной цифровой звукозаписи и подготовки текстов стенограмм мероприятий** Совета Федерации Федерального Собрания РоссийскойФедерации;

- технологических систем обеспечения информационной и документационной

- поддержки заседаний Совета Федерации и Совета палаты на базе автоматизированных рабочих мест членов Совета Федерации в залах заседаний Совета Федерации и Совета палаты.

В настоящий момент ведутся работы по созданию:

- автоматизированной системы обеспечения организационной деятельности, которая должна автоматизировать большинство процессов организации деятельности Совета Федерации;

- корпоративного портала Совета Федерации, который будет объединять корпоративный Интернет/сайт Совета Федерации в качестве информационного ресурса общего доступа и существующие в информационно/коммуникационной системе Совета Федерации информационные ресурсы и обеспечит систему интегрированного поиска, хранения и предоставления информации;

- **Ситуационно/аналитического центра Совета Федерации,** который должен обеспечить повышение эффективности и качества экспертизы последствий принятия законов в социальной, экономической, внешнеполитической и иных сферах, анализа законодательства и правоприменительной практики.

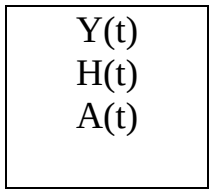
Еще одним достижением в сфере информационного обеспечения деятельности Совета Федерации является обеспечение правового регулирования отношений, возникающих при информационном обеспечении законодательной деятельности, правовыми актами и организационно/распорядительными документами Совета Федерации (распоряжения Председателя Совета Федерации, приказы Руководителя Аппарата Совета Федерации), которые определяют используемые термины, состав и порядок функционирования информационных технологий и информационных систем, порядок поиска, сбора, хранения, обработки, предоставления, распространения информационных ресурсов.

17. Информационно-агрегативная модель государственно-правовой сферы.

Информатизация государственно-правовой сферы призвана улучшить деятельность всех участников законодательного процесса в стране по всему его "жизненному циклу", и прежде всего Федерального Собрания в целом, его палат - Совета Федерации, Государственной Думы, субъектов Российской федерации.

Ниже на рис. 1. приведена информационно-агрегатная модель Федерального Собрания.

Ц(t) П(t) V(t)



W(t) F(t)

Z(t)

R(t) Q(t)

Рис.1. Информационно-агрегатная модель Федерального Собрания РФ

Где:

- **Ц(t)** - краткосрочные, среднесрочные и долгосрочные цели развития страны;
- **ПТ(t)** — программы законодательных инициатив и законопроектных работ, во исполнение которых необходимо разрабатывать законы для обеспечения решения общефедеральных, региональных и местных проблем и формирования пакета целей развития государства;
- **R(t)** - ресурсы, выделяемые государством;
- **W(t)** - возмущения, влияющие на государство и его парламент.
- **Y(t)** — пооперационная системная технология законопроектной работы парламента;
- **H(t)** — процесс непланируемой смены состояний парламента;
- **V(t)** — управляющие решения парламента (законы, постановления, заявления и др.);
- **A(t)** — процесс исполнения управляющих решений;
- **F(t)** - результаты законодательной деятельности парламента;
- **Z(t)** — состояние парламента;
- **Q(t)** — результаты реализации управляющих решений.

Входы и выходы информационного агрегата должны быть заданы соответствующими перечнями разрабатываемых законов, их реквизитами, другими показателями, количественно и качественно характеризующими парламент (палату) или любой другой орган — участник законодательного процесса как объект организационного управления.

№18. Информационно-коммуникационная система Совета Федерации.

Основы Информационно-коммуникационной системы (ИКС), которая позволяет обеспечить наиболее полное , оперативное и качественное информационно-

аналитическое обеспечение СФ и его Аппарата. ИКС разрабатывается с использованием новейших информационных технологий, с учетом имеющегося отечественного и мирового общества.

ИКС должна быть территориально распределенной в силу специфики СФ. Она обеспечивает устойчивое информационное взаимодействие между руководством СФ, комитетами (комиссиями) и членами комитетов, а также между членами СФ и их помощниками.

Работа ИКС должна проводиться в тесном информационном взаимодействии и едином технологическом цикле с аналогичной системой в Государственной Думе. Это позволяет реализовать идею автоматизации законотворчества как многофазного процесса..

ИКС должна охватить все сферы деятельности Совета Федерации, его комитетов и комиссий, структурных подразделений Аппарата.

ИКС станет одной из основных частей единого российского информационного пространства, объединяющего все государственные и не государственные информационные ресурсы, создаваемые органами представительной, исполнительной и судебной власти, коммерческими структурами.

ИКС состоит из множества составляющих, главными из которых являются:

- информационно-справочный центр;
- информационно-коммуникационный центр;
- информационно-аналитический центр;
- ситуационный центр;
- иситема технологического обеспечения заседаний СФ4

……

- центр обучения членов СФ и сотрудников Аппарата.

Цели информатизации Совета Федерации и назначение Информационно-коммуникационной системы.

Информатизация деятельности Совета Федерации направлена на достижение следующих целей:

- повышение эффективности его законотворческой деятельности;
- обеспечение эффективности принятия стратегических решений в штатных и кризисных для страны ситуациях;
- совершенствование взаимодействия Руководства и членов Совета Федерации с гражданами и органами государственной власти;
- повышение эффективности функционирования Аппарата СФ.

Этому и призвана способствовать Информационно-коммуникационная система, выполняющая следующие функции:

- информационное обеспечение деятельности членов СФ, комитетов, комиссий и подразделений Аппарата;
- формирование и ведение информационных фондов;
- информационное взаимодействие (включая электронную почту) членов СФ, комитетов, комиссий и подразделений Аппарата как между собой, так и с внешними абонентами;
- прохождение законодательных актов и законопроектов;
- информационно-аналитическая деятельность Совета Федерации;
- коллективная подготовка и принятие стратегических решений;
- документооборот и делопроизводство;

- редакционно-издательская деятельность;
- доступ пользователей ИКС к информационным фондам и базам данных Совета Федерации, органов государственной власти и организаций РФ, государств СНГ и зарубежных стран;
- офисная деятельность отдельных членов СФ, комитетов, комиссий и подразделений Аппарата;
- технологическое обеспечение заседаний СФ в большом и малых залах;
- информационное обеспечение поездок делегаций СФ и отдельных членов СФ, а также выездных мероприятий СФ.

Основные функциональные подсистемы

В соответствии с классической схемой построения АСУ рассматриваемую нами систему можно представить состоящей из двух основных частей: функциональной и обеспечивающей.

Первая определяется составом и содержанием функциональных подсистем и задач, решаемых в интересах пользователей; вторая — включает техническое, программное, информационное, технологическое и организационное обеспечение.

Состав функциональных подсистем и задач ИКС СФ вытекает из функций Совета Федерации в целом, функций его комитетов, комиссий, структурных подразделений Аппарата, а также определяется сформулированными выше целями информатизации.

Основными функциональными подсистемами ИКС (а их более двух десятков) являются:

Парламентские слушания; Планирование; Законопроект; Заседания Совета Федерации; Законодательство; Делопроизводство; Контроль; Кадры; Аналитика; Статистика; Общественно-политические партии и движения; Регион; Электронные справочники; Выборы; Парламентские процедуры и регламент; Согласительные комиссии; Межпарламентские связи; Материально-техническое обеспечение; Пресс-центр; Содружество Независимых Государств; Комитет по делам Севера и малочисленных народов.

Каждая них, в свою очередь, включает ряд конкретных функциональных задач.

№19. Информационный обмен информацией Российской Федерации в рамках СНГ.

Государства – участники СНГ активно сотрудничают во многих отраслях экономики, науки, техники, политики и других сферах жизнедеятельности. И эффективность здесь в значительной степени зависит от организации информационно обмена данными между государствами Содружества, которые адекватно отображают весь комплекс их двусторонних и многосторонних связей как на государственном уровне, так и между организациями, учреждениями, предприятиями и отдельными гражданами. При этом крайне важно создание в рамках Единого информационного пространства баз данных, характеризующих выполнение взаимных обязательств, достигнутых договоренностей, поручений, соглашений и других решений.

Эффективность двустороннего и многостороннего сотрудничества государств СНГ в большой степени зависит от качества их информационно-аналитического обеспечения по всему комплексу вопросов, относящихся к компетенции совместной деятельности на государственном уровне.

Информация становится не только фундаментом формирующейся информационной инфраструктуры государств, но и продуктом взаимного обмена между государствами СНГ и внешним миром.

Структуру информационного пространства СНГ образуют 12 государств: все бывшие республики СССР за исключением прибалтийских государств.

Как известно, для решения актуальных межгосударственных проблем на уровне СНГ образовано более 160 структур: межпарламентские, межгосударственные, межправительственные координационные и консультационные комиссии, комитеты, советы, рабочие группы и т.п. Ну а если конкретно, то это:

- Совет глав государств СНГ;
- Совет глав правительств;
- Межпарламентская Ассамблея и ряд ее комиссий;
- Статистический комитет СНГ;
- Межгосударственный совет по стандартизации, метрологии и сертификации;
- Межгосударственный координационный совет по научно-технической информации и т.д.

Все эти организации выпускают огромное количество документов, что требует обеспечения возможности своевременного получения этой информации, учета ее, контроля за соответствием и не противоречивостью их друг другу. Ведь все эти вопросы касаются организации совместной деятельности в экономике, в финансовой, таможенной и других сферах деятельности.

Основу информационного пространства СНГ составляют:

- методы, средства и базы данных политической, социально-экономической, правовой и другой государственной информации, которая формируется как на уровне каждого государства Содружества, так и на уровне Содружества в целом. При этом должен обеспечиваться доступ к ним пользователей каждого государства;
- методы и средства автоматизированного сбора, обработки, хранения, передачи и предоставления информации пользователям государств Содружества;

Выполнение этих требований возможно при соблюдении следующих условий: реализации удаленного доступа пользователей СНГ к информационно-коммуникационным ресурсам и вхождения в мировое информационное пространство.

Проблема вхождения в мировое информационное пространство должна решаться по целому ряду направлений:

- необходимо обеспечить внедрение международных стандартов (протоколов) на базе применения технических и программных средств для полной совместимости взаимодействующих информационных систем;
- необходимо обеспечить внедрение международных стандартов и нормативных актов, определяющих правила доступа пользователей разных стран

к информационным ресурсам СНГ и наоборот наших пользователей к их ресурсам;

- необходимо внедрение средств и процедур защиты прав производителей информационной продукции, правил купли-продажи в условиях рыночной экономики и мировых цен.

Такая совместная работа в общем информационном пространстве проводится при соблюдении следующих принципов:

- каждое из государств Содружества обладает национальными информационными ресурсами, которые использует и развивает для решения своих общегосударственных задач;
- информационное пространство СНГ формируется каждым участником как в своих интересах, так и в интересах двустороннего и много стороннего обмена данными на условиях совместного использования;

Существуют некоторые языковые трудности при таком взаимном обмене информацией. Обмен информацией на языках взаимодействующих стран СНГ регулируется в рамках специальных соглашений, определенных национальными информационными центрами. На взгляд специалистов РФ на этапе становления информационного обмена в качестве рабочего языка для описания входных-выходных данных следует признать русский язык.

Соглашения об обмене информацией подписываются главами правительства.

20. Информационный паспорт как средство информационного обслуживания.

Сегодня участникам Межпарламентской Ассамблеи уже недостаточно простого аккумулирования информации о других государствах, а необходимо налаживать тесные контакты между информационными службами стран Содружества. Инициатором в этой части выступает Аппарат Совета Федерации РФ. Там разработана информационно-справочная подсистема «Паспорта государств – участников СНГ».

В качестве сведений о государствах включаются следующие:

- общие сведения;
- политическая система;
- социально-экономическое положение;
- внешняя политика;
- участие в СНГ;
- двусторонние и многосторонние договоры и соглашения с другими государствами – участниками СНГ.

21. Документы, регламентирующие вопросы информационного обмена между странами участниками СНГ.

было принято Положение о порядке получения и использования информации от государств – участников СНГ. В этом документе среди прочих задач поставлена задача о создании автоматизированной системы информационного обмена между государствами Содружества (АСИО СНГ). Концепция АСИО СНГ утверждена Координационно-консультативным Комитетом СНГ 1 марта 1994 г. Схема организации АСИО СНГ включает в себя:

- ИАС г. Москва, которая связана с зарубежными банками данных и системами;
- ситуационный центр и электронный офис Исполнительного Секретариата СНГ в Минске;
- Статистический Комитет СНГ;
- абонентские терминалы государств Содружества;
- информационно-коммуникационный контур, разработанный и сопровождаемый ФАПСИ.

Новой ступенью в процессе расширения и углубления межпарламентской деятельности стало сотрудничество между аппаратами СФ и ГД РФ и Секретариатом ВС Республики Беларусь, меморандум о котором они подписали в Москве 11 апреля 1996 г.

(дополнение): должен состоять из следующих составных частей:

единой (взаимосвязанной) телекоммуникационной сети связи;
единой (взаимосвязанной) системы телеобработки данных;
систем хранения и обработки информации;
систем защиты информации.

22. Информационное обеспечение конгресса США

При конгрессе США существует Исследовательская служба, с которой подписан Меморандум о сотрудничестве между аппаратами СФ и ГД ФС РФ. Кроме нее информационным обслуживанием членов Конгресса занимаются Библиотека Конгресса, коммерческие и правительственные системы, Компьютерный центр Сената, информационные системы палаты представителей.

В числе услуг, предоставляемых ИСК:

- подробный анализ политического курса;
- поиск юридических документов;
- специализированные целевые исследования;
- сотрудники службы проводят семинары и брифинги;
- составляют сравнительный анализ законопроектов;
- составляют библиографические списки;
- подбирают статистические и биографические данные, цитаты, статьи и т.д.

- в их обязанности входит также предоставление индивидуальных услуг в шести читальных залах библиотеки.

Ежегодно силами службы выполняется более полумиллиона заказов Конгресса.

Структура Исследовательской службы Конгресса США

В состав ИСК входят:

- семь исследовательских подразделений;

- два библиотечно-справочных подразделения;

- несколько специализированных бюро.

Информационные системы ИСК США.

1. SCORPIO – информационно-поисковая система, состоящая из много профильных баз данных: по законодательству, по журналам и другим изданиям, книг, карт, опросы общественного мнения, по организациям, и т.д.

2. В дополнение к системе SCORPIO Библиотека Конгресса имеет другие автоматические системы (микрокомпьютерный экранный интерфейс, оптические диски с материалами ИСК, система SDI –избирательное распределение информации, факс-по-требованию).

3. Интернет.

4. Коммерческие и правительственные системы (сельхоз информация, медицина, космос, образование, …).

5. CD-ROM. Конгресс подписывается на них, а библиотека организует доступ к ним в читальных залах.

6. Коммерческие и правительственные данные на лентах/дискетах. Это старая информация, которую нецелесообразно переводить на новые носители. Она требует более длительного периода подготовки.

7. Журналы и книги являются важным источником информации.

8. Телекоммуникационное программное обеспечение для соединения своих компьютеров со службами по каналам связи.

23. Информационное обеспечение парламента Канады

Немалый интерес представляет и опыт информатизации канадского высшего законодательного органа страны, который в своем нынешнем виде существует с 1867 г. Верхняя палата — Сенат состоит из 104 сенаторов, а в Палате общин 295 депутатов. При этом особое внимание уделяется:

- внедрению единых все охватывающих информационных сетей обеих палат,

- электронному безбумажному документообороту,

- электронной системе стенографирования,

- видеоконференциям и т. д.

В Парламенте эксплуатируется информационная система OASIS, объединяющая 14 зданий и осуществляющая обмен информацией на уровнях: голос, видео, данные..

Все PC кабинета подключены к PC-серверу. Таким образом обеспечиваются все три вида услуг: электронная почта, электронное распределение данных (документов), Internet.

Поскольку кабель проложен во все кабинеты зданий, можно оперативно менять конфигурацию рабочих мест с PC. Электронная почта - - база Microsoft — обеспечивает соединение всех зданий Парламента: депутат из своего офиса может послать сообщения во все другие кабинеты.

Депутат связывается с избирательным округом со своего PC, вводит текст и передает сообщение через обычную телефонную линию. Это делается в течение дня, как правило, по нескольку раз. В качестве СУБД используется пакет Access.

Сеть Pubnet предназначена для электронного обмена документами. Это обеспечивает доставку в каждый кабинет электронной версии документа и возможность на каждом рабочем месте на PC печатать из него только то, что нужно. Доступ депутатов к мировым информационным ресурсам осуществляется через сеть Internet, в которой есть база данных "Парламент Канады". В сети Pubnet отслеживается календарь публикаций по дням, а также дебаты, стенограммы выступлений.

Существует телеархив всех выступлений депутатов, можно их повторять с помощью местного TV, позвонив по телефону в студию.

Палата общин заседает 135 дней в году. С учетом такого объема для оперативной подготовки стенограмм привлекаются не только штатные сотрудники, но и студенты.

Внедрена новая технология подготовки публикаций (от диктофонов отказались). Выступления депутатов (до 125—150 человек) в Палате общин в реальном масштабе времени вводятся диспетчером (с наушниками) в специальную

аппаратуру, откуда информация параллельно выбирается на рабочие станции с PC (80—100).

Внутреннее телевидение в Парламенте Канады функционирует с 1977 г. В рамках информационной сети обеспечивается пооперационное сопровождение прохождения проекта закона. В аппарате Комитета трудятся руководитель, секретарь и эксперты по найму.

В Сенате создана своя сеть (на базе Ethernet), к которой подключены все 450 PC. В ней пять серверов, объединяющих пять зданий. 70% ремонта PC осуществляет группа из трех-четырех человек, остальные работы ведутся с привлечением других организаций.

Информационная система Палаты общин действует с ноября 1994 г. Для связи с округами депутат использует личный Internet, за что он платит 20 долларов в месяц за 50 часов работы. У каждого депутата — свой бюджет, своя комната в Парламенте. Он имеет помощников (6 и более), работающих по делам округа. Депутат печатается бесплатно, четыре раза в год он может посылать в округ материалы бесплатно.

Значительное внимание уделяется связям Парламента с общественностью. Для этого на запросы извне информация выдается по телефону.

В фондах парламентской библиотеки насчитывается 650 тыс. книг на английском и французском языках, пришло несколько книг из России.

В Парламенте Канады внедрена система телеконференций.

24. Информатизация управления европейских структур.

Европейский Союз призван рассматривать проблемы, которые трудно, а зачастую просто невозможно объективно разрешить на национальном уровне. Орган управления Евросоюза состоит из семи подразделений:

- Совет Министров;
- Европейский Совет;
- Европейская Комиссия;
- Европейский Парламент;
- Комитет по экономике и социальной политике;
- Судебная палата;
- Аудиторская палата.

Информационно-коммуникационная система Европарламента — это сложный программно-технический комплекс. Система базируется на разнородной аппаратной платформе семи ведущих фирм. В качестве основной принята СУБД Oracle. Система ориентируется на работу в режиме клиент-сервер. Каких-то веских причин выбора именно этой СУБД высказано не было.

Информационная служба Европейской Комиссии

Стратегия Директората информационных технологий -- открытые системы: UNIX-серверы, Windows -- рабочие станции, СУБД Oracl RDBMS, текстовый редактор (WordPerfect). Считают целесообразным работать на различных аппаратных
платформах: Olivetty, Siemens, Sun, DEC, Bull, ICL, NCR.
Комиссия размещается в 53 зданиях в Брюсселе, четырех зданиях в Люксембурге и в 15 зданиях в Испре (Италия). Коммуникационный центр располагается в Брюсселе. Связь между Брюсселем и Люксембургом осуществляется по двум 2МБ- и одному 64-кб каналам связи, между Люксембургом и Италией — по трем 64-кб каналам связи. Главный компьютерный центр расположен в Люксембурге. Рассылка документов осуществляется следующим образом: документы переводятся на все языки в Брюсселе и помещаются в базу данных; доступ к документам - с помощью программы CELLEX. Копия каждого документа рассылается всем адресатам и на бумажном носителе. СУБД Oracle сегодня внедрена только в половине директоратов и работает в режиме клиент-сервер.

Информационная служба Европарламента

Возглавляет аппарат Европарламента Генеральный секретарь, в подчинении которого находятся:

- директорат информационных технологий (100 человек),

Структура Директората информационных технологий

Директорат информационных технологий подчиняется Генеральному секретарю Европарламента и включает в себя:

1. Административный отдел (10 человек)
2. Отдел информатизации: компьютерный центр (10 человек); разработка систем на Main Frame (30 человек); поддержка пользователя и автоматизация офиса (30 человек); отношения между различными институтами (10 человек).
3. Отдел организации и методологии (10 человек).
4. Телекоммуникационный отдел: сетевое обеспечение (15 человек); удаленный доступ (30 человек).

В качестве центральной машины Компьютерного центра
используется Main Frame фирмы IBM, серверы баз данных и приложений работают на HP9000 и Sun, файловые и почтовые серверы — Olivetty, BULL. На центральной машине развернута СУБД A DABAS, на локальных серверах
— Oracle под управлением UNIX, на рабочих станциях -- Paradox под управлением Windows.

Евростат

Основные приложения Евростата написаны на Oracle и предназначены для регистрации почты, архивации на оптических дисках, заказа оборудования, управления внутренними проектами, общих информационных систем (бюджет, отчеты о командировках, оплата работ). Oracle-сервер работает на Sun. В настоящее время в сети — пять серверов, в будущем предполагается оставить только три. Приложения работают в режиме клиент-сервер.

Государственный центр информатики (Люксембург)

Он занимается как разработкой приложений на уровне предприятий и отдельных заказчиков, так и эксплуатацией (управление из Центра, закупка,

поддержка систем и оборудования). В эксплуатации находится 180 приложений (23 800 программ и 8600 баз данных), 10 приложений разрабатываются
В ряду наиболее известных проектов можно отметить следующие:
1. институт вина — контроль размещения и качества;
2. Шенгенская информационная система — служба безопасности Евросоюза, криминальная информация;
3. гражданская оборона — контроль состояния воды в реках;
4. приложения для полиции Люксембурга, где задействованы 80 UNIX-серверов. Разрабатывается проект единой системы для Европы, предполагающий использование в качестве центральной СУБД — СУБД DB2, функционирующую на Main Frame, и локальные UNIX-серверы с СУБД Oracle;
5. геоинформационная система;
6. экология;
7. управление территориями;
8. медицина.

25. Развитие информационных технологий в парламентах государств Европы.

Конференция "Информационные технологии в парламентах"

20—22 июня 1994 г. Присутствовали представители информационных, технических и технологических служб парламентов Великобритании, Испании, Италии, Швеции, Финляндии, Германии, Польши, Венгрии, Чехии, Словакии, Болгарии, Македонии, Румынии, Беларуси, Украины, Эстонии, Литвы, Латвии, России, Европарламента; в качестве гостей присутствовали представители служб Конгресса США и Целевого фонда, возглавляемого сенатором Мартином Фростом (США).
Обсуждались:
проведение заседаний;
архитектура информационных систем;
организация телекоммуникационного взаимодействия;
организация создания и ведения полнотекстовых баз данных (БД).
На заседаниях практически во всех парламентах используется электронная система голосования. В ряде систем отсутствует табло результатов голосования, а компьютерная распечатка передается председательствующему для оглашения. + технологическое TV для отображения справочной информации о повестке дня заседания, ходе заседания, результатах обсуждения вопросов и т. п. Электронная система голосования связана с информационной системой парламента для пересылки результатов голосования на файл-сервер центральной базы данных для их хранения..
В ряде парламентов в состав информационной системы входит информационное звено на базе высокопроизводительной ЭВМ (Main Frame) различных фирм -- Siemens, DDS, VAX, SVN, IBM. Базы данных информационной системы размещаются на нескольких файл-серверах (от двух до восьми) с объемом памяти

1 = 15 Гб в соответствии с тематической принадлежностью хранимой информации, чтобы уменьшить время доступа конечного пользователя.
Средства телекоммуникации, обеспечивающие удаленное взаимодействие (интерактивный доступ к БД и электронная почта) с офисами парламентариев на местах, правительственными и государственными учреждениями, в основном строятся на использовании внутригосударственных коммутируемых телефонных сетей X.25.
Выход в каждый из типов связей обеспечивается через отдельный коммуникационный сервер или факс-сервер. Определяющей перспективой здесь является выход на спутниковые каналы связи.
Для создания и ведения полнотекстовых баз данных широкое распространение получило применение сканеров для ввода текстовых документов, программных средств распознавания образов (OCR) и оптических дисков (CD-ROM).

Семинар "Информационные и коммуникационные технологии в парламентах"

16—18 октября 1995 г. в г. Берне. Участие - 58 представителей парламентских служб 30 европейских стран, а также информационных служб Совета Европы и Европарламента.
Наряду с представителями Беларуси, Чехии, Эстонии, Финляндии, Германии, Венгрии, Испании, Италии, Македонии, Польши, Румынии, России, Словакии, Украины, Великобритании, участвовавшими в упоминавшемся нами семинаре в Польше, здесь были представлены также Албания, Бельгия, Хорватия, Дания, Франция, Исландия, Ирландия, Лихтенштейн, Мальта, Молдова, Голландия, Норвегия, Словения, Швейцария.
Основные тенденции использования информационных ресурсов и информационных технологий для поддержки законотворческого процесса и повседневной деятельности парламентариев и обеспечивающих их работу служб.
В ряде парламентов функционируют автоматизированные системы контроля прохождения законопроектов, позволяющие получать информацию о том, на какой стадии находится конкретный законопроект, а также документы, сопровождающие этот законопроект, и интересующую интегральную статистическую информацию по совокупности законопроектов, находящихся в обсуждении, принятых или отклоненных на различных этапах законодательной процедуры, контролировать сроки отдельных таких этапов.
Возможность оперативного удаленного взаимодействия парламентариев базируется на государственных телефонных сетях (технология ISDN), обеспечивающих передачу цифровых данных, голоса, изображения, факсов.
Практически парламенты всех стран имеют выход в инет. В парламенте Исландии доступ к информационным ресурсам реализован на принципах с использованием программных продуктов сети INTERNET. В парламентах некоторых стран (Германия, Венгрия, Словения) внедрены WWW-серверы (World Wide Web Server) этой сети, информация на которых обновляется еженедельно. Ряд парламентов планирует внедрение WWW-серверов в ближайшем будущем. Однако следует отметить, что в настоящее время информация WWW-серверов представляется на государственных языках, что

резко снижает количество пользователей в мире, которые могут использовать эту информацию.

В последнее время широкое распространение получили информационные технологии с использованием носителей CD-ROM: для архивирования текстовых баз данных, создания аудиодисков CD-ROM с записью выступлений парламентариев на заседаниях, для поиска необходимой информации по реквизитам.

Межпарламентский семинар по информационным технологиям и коммуникациям

Прага 7—9 октября 1996 г. под эгидой Европейского центра парламентских исследований и документации (ECPRD), целью которой является укрепление связей между информационными службами парламентов стран Европы, обмен опытом по использованию новых информационных технологий обеспечения законодательного процесса, пропаганда деятельности парламента.

Использование сети Интернет для освещения деятельности парламентов.

- В парламенте *Чешской Республики* формировалась единая компьютерная сеть в течение 6 лет.

В начале 1996 г. был создан web-сервер в сети Интернет (www.psp.cz), содержащий следующую информацию:

— структура парламента;

— председатель парламента и его заместители;

- члены парламента (анкетные данные, работа в парламенте, данные о голосовании);

- законодательная деятельность.

Информация на сервере представлена на четырех языках (чешском, немецком, французском и английском) и в полном объеме доступна как внутренним, так и внешним пользователям по принципу "нет секретов от народа".

Румыния ориентируется на страны Черноморского сообщества и Европарламент

На тот период сеть сената парламента объединяла 55 рабочих станций и три сервера.

В числе нерешенных проблем назывались следующие:

- Во-первых, подготовка документов на нескольких языках требует больших финансовых затрат, между тем в работе с Европарламентом используется английский язык. Поэтому в мае 1996 г. проводился опрос парламентариев по поводу использования второго языка для внешнего общения, и каждый второй член парламента выбрал английский.

- Во-вторых, не было еще выхода в сеть Internet.

В ближайшем будущем планируется создание сети, объединяющей локальные сети комитетов, обе палаты парламента, парламентскую библиотеку с сервером в сети Интернет.

Парламент *Болгарии* работает в двух зданиях, соединенных компьютерной сетью типа Ethernet и выходом в сеть Интернет через коммуникации Академии наук Болгарии. В то время в сети Интернет пользователям парламента доступен был только режим электронной почты.

Большое значение придается обмену законодательной информацией с парламентами стран Европы с использованием законодательных БД CELEX, JUSTIS, LEXIS на CD-ROM.
Перспективы:
- прямой выход в Интернет;
— создание web-сервера Национального Собрания Болгарии;
- использование оптико-волоконного кабеля для соединения парламента с Советом Министров и президентскими структурами.
Все компьютеры Национального Собрания *Франции* объединены в сеть, к которой осуществляется доступ внешних пользователей. На сервере размещены БД парламента, индивидуальные информационные страницы членов парламента. Базы данных содержат материалы заседаний, исторические справки о парламенте, отчеты об основных событиях. Эта информация оперативно поступает на сервер и вызывает большой интерес у журналистов и пользователей из провинций.
По соображениям безопасности доступ к серверу ограничен, он не имеет выхода в сеть Интернет, что вызывает неудовольствие членов парламента.
Если говорить о перспективах, то они связываются с телеконференциями и выходом в сеть Интернет.
К проблемам можно отнести следующее:
— недостаточное финансирование;
- не все парламентарии свободно работают на компьютере;
— необходимость обеспечить безопасность (программные и технические средства защиты).
Парламент *Швеции* ориентирован на использование системы работы с текстовыми документами Rixlex, доступ к которой осуществляется в сети Internet в режиме Telnet и только пользователями внутри страны.
Информация парламента предоставляется бесплатно, до июля 1996 г. такая возможность предоставлялась только библиотекам.
БД парламента содержат следующую информацию:
- история законодательства, исторические документы;
— о парламенте;
— комитеты;
— законотворческая деятельность;
— правительство;
— парламентская библиотека;
— документы международных организаций Европейского сообщества.
Достоинство системы Rixlex заключается в возможности поиска информации в нескольких базах данных одновременно.
На перспективу намечены:
- организация web-сервера;
- проведение работ по проекту Elvil — европейская законодательная виртуальная библиотека, включающая создание общего интерфейса, использование средств мультимедиа для представления информации.
Парламент Финляндии начал использовать компьютерную технику с 1987 г. После межпарламентского семинара в Польше в 1993 г., проанализировав опыт

информационных служб парламентов разных стран, решили строить систему информационного обеспечения депутатов парламента с использованием принципов сети Интернет, достоинствами которой являются экономичность, простота технического решения, удобный интерфейс.

Членам парламента обеспечен доступ к web-серверу внутренней сети парламента, имеющей выход в сеть Интернет через фильтр зашиты. Для внешних пользователей организован web-сервер в сети Интернет (www.eduskunta.fi), на который копируется открытая информация с внутреннего сервера. Два web-сервера были созданы с целью обеспечения безопасности внутренней сети.

Парламентариям как пользователям этой сети, в том числе и с компьютеров notebook из любой точки мира, предоставляются следующие возможности:

— электронная почта;

- доступ в сеть Интернет;

- доступ к информации парламента и правительства (календарь событий, тексты документов, отчеты комитетов, законопроекты и т. д.);

— доступ к архивным документам;

— библиотечные каталоги;

- доступ к БД информационных агентств.

Каждая **палата парламента Германии** имеет свою внутреннюю информационную сеть, обеспечивающую деятельность депутатов, без доступа для внешних пользователей. Верхняя палата, используя свои технические возможности, организовала web-сервер в сети Internet, содержащий информацию о деятельности палаты и материалы агентств на немецком языке.

Ведутся работы по объединению двух палат парламента и правительства в единую информационную сеть с выходом в Internet. Такое решение считается наиболее эффективным с точки зрения экономичности и технического обеспечения.

Информационно-технологический отдел палаты депутатов **парламента Италии** занимается изучением, планированием и развитием информационных и технических ресурсов палаты. 69 согрудников обеспечивают работу 1000 компьютеров, объединенных в сеть, и шести серверов.

В стадии решения — проблемы использования системы звукового распознавания для ведения стенограмм заседаний палаты и слушаний в комитетах.

В будущем планируется объединить сети парламента и правительства.

В связи с ростом популярности сети Интернет, увеличением количества серверов в сети, числа хакеров и коммерческим использованием сети Интернет важное значение приобретает вопрос о безопасности сети и защите данных на сервере.

И здесь существуют разные способы защиты:

— использование только выделенных каналов;

— все каналы должны быть со средствами защиты;

- использование только лицензированного программного обеспечения.

В то же время практика показывает, что установка пароля для доступа к данным отнюдь не эффективное средство защиты.

Более подробно проблемы безопасности информации, связанные с подключением к сети Интернет, были рассмотрены на семинаре осенью 1997 г. в Риме.
В настоящее время парламенты 23 европейских государств имеют web-серверы в сети

26. Понятие информационной безопасности ИС. Виды угроз информационной безопасности.

Развитие информационных технологий и всеобщая компьютеризация привели к тому, что информационная безопасность не только становится обязательной, она еще и одна из характеристик.
Под *безопасностью ИС* понимается защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, от попыток хищения (несанкционированного получения) информации, модификации или физического разрушения ее компонентов.
Под *угрозой безопасности информации* понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Среди угроз безопасности информации следует выделять *случайные (непреднамеренные) и умышленные*.
Источниками случайных видов угроз могут быть:
- выход из строя аппаратных средств;
- неправильные действия работников ИС или ее пользователей;
- непреднамеренные ошибки в программном обеспечении и т.д.

Умышленные виды угрозы преследуют цель нанесения ущерба управляемой системе или пользователям. Часто это делается ради получения личной выгоды.
В настоящее время для обеспечения защиты информации требуется не просто разработка частных механизмов защиты, а реализация системного подхода. Сегодня можно смело утверждать, что рождается новая современная технология – *технология защиты информации* в компьютерных информационных системах и сетях передачи данных. Реализация этой технологии требует увеличивающихся расходов и усилий, однако, это позволяет избежать значительно превосходящих потерь и ущерба, которые могут возникнуть при реальном осуществлении угроз ИС и ИТ.

Виды угроз информационной безопасности

Можно по разному классифицировать виды угроз:
- *пассивные и активные;*
- *внутренние и внешние;*

Пассивные угрозы направлены в основном на несанкционированное пользование ресурсами системы, не оказывая при этом на нее влияния (прослушивание каналов связи, просмотр БД, …).
Внешние угрозы могут определяться злонамеренными действиями конкурентов, изменением экономических условий, стихийными бедствиями.

К основным угрозам безопасности информации и нормального функционирования ИС относятся:

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

27. Принципы, на которых основано создание систем информационной безопасности.

Создание систем информационной безопасности (СИБ) в ИС и ИТ основывается на следующих принципах:

- *Системный подход* к построению системы защиты, означающий оптимальное сочетание организационных, программных, аппаратных, физических подсистем.
- *Принцип непрерывного развития системы*. Обеспечение безопасности ИС не может быть одноразовым актом. Непрерывно совершенствуются способы и реализации угроз, и борьбы с ними.
- *Разделение и минимизация полномочий* по доступу к обрабатываемой информации и процедурам обработки.

Полнота контроля и регистрации попыток несанкционированного доступа. Имеется в виду полная идентификация каждого пользователя и протоколирования его действий, а также невозможность совершения любой операции без ее регистрации.

- *Обеспечение надежности системы защиты*, невозможность снижения уровня защиты при возникновении в системе сбоев, преднамеренных действий взломщика или непреднамеренных ошибок персонала.,
- *Обеспечение контроля за функционированием системы защиты*, т.е. создание средств и методов контроля работоспособности механизмов защиты.
- *Обеспечение всевозможных средств борьбы с вредоносными программами.*
- *Обеспечение экономической целесообразности использования систем защиты*. Стоимость разработки и эксплуатации СИБ не должна превышать возможного ущерба при реализации угроз.

28. Методы и средства обеспечения информации в системах информационной безопасности.

Под *безопасностью ИС* понимается защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, от попыток хищения (несанкционированного получения) информации, модификации или физического разрушения ее компонентов.

Системы защиты и этапы их разработки

Состояние защищенности ИС должно характеризоваться показателем защищенности. Под *показателем защищенности* будем понимать характеристику средств системы, влияющую на защищенность и описываемую определенной группой требований.

Подход к защищенности и к оценкам безопасности одинаков и в США и в России.

Вопросами стандартизации и разработки нормативных требований на защиту информации в США занимается Национальный центр компьютерной безопасности министерства обороны США (NCSC – National Computer Security Center). В 1985 г.были утверждены критерии безопасности. Этот документ называется Оранжевая книга.

В оранжевой книге приведены четыре уровня безопасности компьютерных систем:

- A, высший класс;
- B, промежуточный;
- C, низкий уровень безопасности;
- D, класс систем, не прошедших испытания.

В России роль Национального Центра Компьютерной Безопасности играет Государственная техническая комиссия при Президенте РФ, а роль Оранжевой книги Руководящий документ госкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации», выпущенная в 1992 г. В России принята семи-уровневая система защиты информации

Создание систем информационной безопасности (СИБ) в ИС и ИТ основывается на следующих принципах:

- *Системный подход* к построению системы защиты, означающий оптимальное сочетание организационных, программных, аппаратных, физических подсистем.
- *Принцип непрерывного развития системы*. Обеспечение безопасности ИС не может быть одноразовым актом. Непрерывно совершенствуются способы и реализации угроз, и борьбы с ними.
- *Разделение и минимизация полномочий* по доступу к обрабатываемой информации и процедурам обработки.
- *Полнота контроля и регистрации попыток* несанкционированного доступа. Имеется в виду полная идентификация каждого пользователя и протоколирования его действий, а также невозможность совершения любой операции без ее регистрации.
- *Обеспечение надежности системы защиты*, невозможность снижения уровня защиты при возникновении в системе сбоев, преднамеренных действий взломщика или непреднамеренных ошибок персонала.,
- *Обеспечение контроля за функционированием системы защиты*, т.е. создание средств и методов контроля работоспособности механизмов защиты.
- *Обеспечение всевозможных средств борьбы с вредоносными программами.*
- *Обеспечение экономической целесообразности использования систем защиты*. Стоимость разработки и эксплуатации СИБ не должна превышать возможного ущерба при реализации угроз.

Методы и средства обеспечения безопасности информации в СИБ включают в себя:

- *Препятствие* метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, к нсителям и т.д.).
- *Управление доступом* – (идентификация пользователей, опознание объекта-субъекта, проверка полномочий, разрешение и создание условий работы в пределах установленного регламента, регистрация обращений к защищаемым ресурсам, реагирование на попытки несанкционированных действий).
- *Механизм шифрования* – криптографическое закрытие информации.
- *Противодействие атакам вредоносных программ* – использование АВП,
- *Регламентация* - создание условий обработки информации с наибольшим соблюдением спецтребований.
- *Принуждение* - метод защиты, при котором персонал вынужден работать с соблюдением требований безопасности.
- *Побуждение* – метод защиты, при котором сами пользователи стараются не нарушать меры безопасности.
- *Аппаратные средства* – спецустройства, подключаемые в ВТ для обеспечения безопасности.
- *Физические средства* – (замки на дверях, решетки на окнах, охранная сигнализация и т.д.).
- *Программные средства* – спецпрограммы, включая криптографические.
- *Организационные средства* – Комплекс организационных мероприятий, способствующих обеспечению безопасности информации при обработке ее в ИС разрабатывается и реализуется службой информационной безопасности.
- *Законодательные средства* защиты определяются законодательными актами страны
- *Морально-этические средства* включают всевозможные меры поведения, традиционно сложившиеся ранее. Морально-этические нормы могут быть писаные (устав) и неписаные (честность). Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ в США.
- Функции Аудиторской палаты сводятся главным образом к контролю финансовой стороны процессов. В ее составе 12 специалистов, 1000 штатных сотрудников. Территориально подразделения Евросоюза размещаются следующим образом:
- Совет Министров - - Брюссель;
- Комиссия - - Брюссель, Люксембург, Испра (Италия);
- Европарламент — административная работа проходит в Брюсселе и Люксембурге, а заседания — в Страсбурге;
- Комитет по экономике и социальной политике базируется в Брюсселе;
- Судебная и Аудиторская палаты — в Люксембурге.
-
- Весь документооборот ведется на девяти языках: французском, немецком, итальянском, голландском, датском, английском, испанском, португальском и греческом. СУБД Oracle поддерживает все эти языки. В ближайшее время планируется включение финского и шведского языков.

Особенности защиты информации в сетях

Системы информационной безопасности сетей значительно сложнее, чем в случае автономной обработки информации.

Архитектурную концепцию системы защиты информации в сетях можно представить в виде трех слоев:

- средства защиты сетевого уровня;
- middleware-системы (транспортный, сеансовый и уровень представлений);
- средства защиты, предлагаемые прикладными программами

Построение СИБ сети основано на семиуровневой модели декомпозиции системного управления OSI/ISO. ISO – Международная организация по стандартизации, а OSI – стандарты взаимодействия открытых систем. Так вот они выделяют семь уровней сетевой архитектуры, которая обеспечивает передачу и обработку информации в сети. Семь уровней сетевого управления включают в себя: физический, канальный, сетевой, транспортный, сеансовый, представительский, прикладной уровни.

Следует отметить, что использование протокола TCP/IP решает задачу обеспечения безопасности с любым необходимым уровнем надежности.

29. Системы защиты информации в США

Возрастание роли информационных ресурсов в конкурентной борьбе, внедрение ИТ в сферу финансово-денежных отношений, всеобщая компьютеризация, широкое использование коммуникационных сетей привели к тому, что информационная безопасность становится обязательной практически для любой ИС. Дело в том, что информация, обращающаяся в них, может быть незаконно изменена, похищена или уничтожена. Поэтому главной проблемой, которую должны решить разработчики при создании системы защиты ИС, является проблема обеспечения безопасности хранимых данных, предусматривающая разработку комплекса мер обеспечения безопасности, направленных на предотвращение несанкционированного получения информации, физического ее уничтожения или изменения. Вопросы разработки способов и методов защиты данных являются только частью проблемы проектирования системы защиты в ИС.

Для обеспечения защиты информации требуется не только разработка частных механизмов защиты, а реализация системного подхода, включающего комплекс взаимосвязанных мероприятий (применение специальных технических и программных средств, организационных мер, нормативно-правовых актов, морально-этического воспитания и т.д.). Комплексный характер защиты проистекает из комплексных действий «компьютерных пиратов» (хакеров), стремящихся любыми средствами добыть важную для них информацию.

· ***Препятствие*** – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

· ***Управление доступом*** – метод защиты информации регулированием использования ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации. Управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора: кода, пароля и т.д.);
- аутентификацию – установление подлинности объекта или субъекта по предъявленному им идентификатору;
- авторизацию – проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- разрешение и создание условий работы в пределах установленного регламента;
- регистрацию (протоколирование) обращений к защищенным ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.д.) при попытках несанкционированных действий.

· ***Механизмы шифрования*** – криптографическое закрытие информации. Для реализации мер безопасности используют различные способы шифрования (криптографии), суть которых заключается в том, что данные, отправляемые на хранение, или сообщения, готовые к передаче, зашифровываются, т.е. преобразуются в шифрограмму или закрытый текст. Санкционированный пользователь получает данные (сообщение), дешифрует их или раскрывает посредством обратного преобразования криптограммы, в результате чего получается исходный открытый текст. Этот способ является надежным при передаче информации по каналам большой протяженности.

· ***Противодействие атакам вредоносных программ*** – предполагает комплекс мер организационного характера и использование антивирусных программ.

· ***Регламентация*** – создание таких условий автоматизированной обработки, хранения и передачи защищаемой информации, при которых нормы и стандарты по защите выполняются в наибольшей степени.

· ***Принуждение*** – метод защиты, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

· ***Побуждение*** – метод защиты, побуждающий пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Вся совокупность технических средств подразделяется на аппаратные и физические.

· ***Аппаратные средства*** – устройства, встраиваемые непосредственно в компьютер, или устройства, которые сопрягаются с ним по стандартному интерфейсу.

· ***Физические средства*** – включают инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты (замки, решетки, средства электронной охранной сигнализации и т.п.).

· ***Программные средства*** – это специальные программы, предназначенные для защиты информации в ИС. Здесь выделяются еще программные средства, реализующие механизмы шифрования (криптографии).

Криптография – это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

· ***Организационные средства*** – осуществляют регламентацию производственной деятельности в ИС и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становятся невозможными или существенно затрудняются. Комплекс этих мер реализуется группой информационной безопасности.

· ***Законодательные средства*** защиты определяются законодательными актами государства, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

· ***Морально-этические средства*** защиты включают нормы поведения, которые складываются по мере развития ИС и ИТ в стране и в мире или специально разрабатываются. Морально-этические нормы могут быть неписаные, например честность, либо оформленные в некий свод (устав) правил организации.

Архитектурная концепция системы защиты информации в сетях представляется в виде трех слоев: средства защиты сетевого уровня, middleware-системы и средства защиты, предлагаемые прикладными системами.

Самым распространенным методом установления подлинности служит метод *паролей*.

Пароль представляет собой строку символов, которую пользователь должен ввести в систему. Если введенный пароль соответствует паролю, хранящемуся в памяти компьютера, то пользователь получает доступ ко всей информации, защищенной этим паролем. Пароль можно использовать и независимо от пользователя для защиты БД, файлов, записей и т.д. Укажем некоторые виды паролей.

1. ***Простой пароль***. Пользователь вводит ряд символов с клавиатуры после запроса, а компьютерная программа (или специальная микросхема) кодирует его и сравнивает с хранящимся в памяти эталоном. Простой пароль рекомендуется применять для защиты малозначимых данных.
2. ***Пароль однократного использования***. Пользователю выдается список из нескольких паролей, которые хранятся в памяти компьютера в зашифрованном виде. После использования пароль стирается из памяти и вычеркивается из списка, так что перехват пароля теряет смысл. Такой пароль обеспечивает более высокую степень безопасности, но более сложен.
3. ***Пароль на основе выборки символов***. Пользователь выводит из пароля отдельные символы, позиции которых задаются, например, с помощью генератора псевдослучайных чисел.
4. ***Метод «запрос-ответ».*** Пользователь должен дать правильные ответы на набор вопросов, хранящихся в памяти компьютера и управляемых операционной системой. Иногда пользователю задается много вопросов, и он может сам выбрать те из них, на которые он желает ответить.
5. ***Пароль на основе алгоритма***. Пароль определяется на основе алгоритма, который хранится в памяти компьютера и известен пользователю. Система

выводит на экран случайное число, и пользователь, с одной стороны, а компьютер – с другой, на его основе вычисляют по известному алгоритму пароль. Этот способ обеспечивает более высокую степень безопасности, чем многие другие, но требует дополнительных затрат времени пользователя.

Пароли широко применяются при защите информации. Они просты и дешевы при реализации, однако парольной защиты не всегда бывает достаточно для обеспечения безопасности ИС.

30. Системы защиты информации в РФ.

Возрастание роли информационных ресурсов в конкурентной борьбе, внедрение ИТ в сферу финансово-денежных отношений, всеобщая компьютеризация, широкое использование коммуникационных сетей привели к тому, что информационная безопасность становится обязательной практически для любой ИС. Дело в том, что информация, обращающаяся в них, может быть незаконно изменена, похищена или уничтожена. Поэтому главной проблемой, которую должны решить разработчики при создании системы защиты ИС, является проблема обеспечения безопасности хранимых данных, предусматривающая разработку комплекса мер обеспечения безопасности, направленных на предотвращение несанкционированного получения информации, физического ее уничтожения или изменения. Вопросы разработки способов и методов защиты данных являются только частью проблемы проектирования системы защиты в ИС.

Для обеспечения защиты информации требуется не только разработка частных механизмов защиты, а реализация системного подхода, включающего комплекс взаимосвязанных мероприятий (применение специальных технических и программных средств, организационных мер, нормативно-правовых актов, морально-этического воспитания и т.д.). Комплексный характер защиты проистекает из комплексных действий «компьютерных пиратов» (хакеров), стремящихся любыми средствами добыть важную для них информацию.

· *Препятствие* – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

· *Управление доступом* – метод защиты информации регулированием использования ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации. Управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора: кода, пароля и т.д.);
- аутентификацию – установление подлинности объекта или субъекта по предъявленному им идентификатору;
- авторизацию – проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

- разрешение и создание условий работы в пределах установленного регламента;
- регистрацию (протоколирование) обращений к защищенным ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.д.) при попытках несанкционированных действий.

· *Механизмы шифрования* – криптографическое закрытие информации. Для реализации мер безопасности используют различные способы шифрования (криптографии), суть которых заключается в том, что данные, отправляемые на хранение, или сообщения, готовые к передаче, зашифровываются, т.е. преобразуются в шифрограмму или закрытый текст. Санкционированный пользователь получает данные (сообщение), дешифрует их или раскрывает посредством обратного преобразования криптограммы, в результате чего получается исходный открытый текст. Этот способ является надежным при передаче информации по каналам большой протяженности.

· *Противодействие атакам вредоносных программ* – предполагает комплекс мер организационного характера и использование антивирусных программ.

· *Регламентация* – создание таких условий автоматизированной обработки, хранения и передачи защищаемой информации, при которых нормы и стандарты по защите выполняются в наибольшей степени.

· *Принуждение* – метод защиты, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

· *Побуждение* – метод защиты, побуждающий пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Вся совокупность технических средств подразделяется на аппаратные и физические.

· *Аппаратные средства* – устройства, встраиваемые непосредственно в компьютер, или устройства, которые сопрягаются с ним по стандартному интерфейсу.

· *Физические средства* – включают инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты (замки, решетки, средства электронной охранной сигнализации и т.п.).

· *Программные средства* – это специальные программы, предназначенные для защиты информации в ИС. Здесь выделяются еще программные средства, реализующие механизмы шифрования (криптографии). Криптография – это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

· *Организационные средства* – осуществляют регламентацию производственной деятельности в ИС и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становятся

невозможными или существенно затрудняются. Комплекс этих мер реализуется группой информационной безопасности.

· *Законодательные средства* защиты определяются законодательными актами государства, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

· *Морально-этические средства* защиты включают нормы поведения, которые складываются по мере развития ИС и ИТ в стране и в мире или специально разрабатываются. Морально-этические нормы могут быть неписаные, например честность, либо оформленные в некий свод (устав) правил организации.

Архитектурная концепция системы защиты информации в сетях представляется в виде трех слоев: средства защиты сетевого уровня, middleware-системы и средства защиты, предлагаемые прикладными системами.

Самым распространенным методом установления подлинности служит метод *паролей.*

Пароль представляет собой строку символов, которую пользователь должен ввести в систему. Если введенный пароль соответствует паролю, хранящемуся в памяти компьютера, то пользователь получает доступ ко всей информации, защищенной этим паролем. Пароль можно использовать и независимо от пользователя для защиты БД, файлов, записей и т.д. Укажем некоторые виды паролей.

1. *Простой пароль.* Пользователь вводит ряд символов с клавиатуры после запроса, а компьютерная программа (или специальная микросхема) кодирует его и сравнивает с хранящимся в памяти эталоном. Простой пароль рекомендуется применять для защиты малозначимых данных.
2. *Пароль однократного использования*. Пользователю выдается список из нескольких паролей, которые хранятся в памяти компьютера в зашифрованном виде. После использования пароль стирается из памяти и вычеркивается из списка, так что перехват пароля теряет смысл. Такой пароль обеспечивает более высокую степень безопасности, но более сложен.
3. *Пароль на основе выборки символов*. Пользователь выводит из пароля отдельные символы, позиции которых задаются, например, с помощью генератора псевдослучайных чисел.
4. *Метод «запрос-ответ»*. Пользователь должен дать правильные ответы на набор вопросов, хранящихся в памяти компьютера и управляемых операционной системой. Иногда пользователю задается много вопросов, и он может сам выбрать те из них, на которые он желает ответить.
5. *Пароль на основе алгоритма*. Пароль определяется на основе алгоритма, который хранится в памяти компьютера и известен пользователю. Система выводит на экран случайное число, и пользователь, с одной стороны, а компьютер – с другой, на его основе вычисляют по известному алгоритму пароль. Этот способ обеспечивает более высокую степень безопасности, чем многие другие, но требует дополнительных затрат времени пользователя.

Пароли широко применяются при защите информации. Они просты и дешевы при реализации, однако парольной защиты не всегда бывает достаточно для обеспечения безопасности ИС.