Московский государственный технический университет
имени Н.Э. Баумана

В.М. Постников

Основы эксплуатации АСОИиУ
Том 2
Администрирование и развитие АСОИиУ

Допущено Учебно-методическим объединением вузов Российской Федерации по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению подготовки 230100 «Информатика и вычислительная техника»

Москва
Издательство МГТУ им. Н.Э. Баумана
2015

УДК 004(075.8)
ББК 22.18я73
П63

Рецензенты:
зав. кафедрой «Информационные системы в экономике и управлении НОУ ВПО» Российский новый университет, д-р, техн. наук, профессор Л.В. Лабунец,
д-р техн. наук, профессор кафедры «Автоматизированные системы управления» Московского автомобильно-дорожного государственного технического университета (МАДИ) П.Ф. Юрчик

Постников В. М.

П63 Основы эксплуатации АСОИиУ. Том 2. Администрирование и развитие АСОИиУ: 2-е издание переработанное и дополненное, учеб. пособие / В. М. Постников. — М.: Изд-во МГТУ им. Н. Э. Баумана, 2015. — 205, [2] с.: ил.

ISBN 978-5-7038-3655-2

Рассмотрены основные понятия, методы, подходы, нормативные и руководящие материалы, необходимые обслуживающему персоналу при проведении работ по эксплуатации автоматизированных систем обработки информации и управления, построенных на основе современных локальных вычислительных сетей. Содержится большое количество примеров, практических советов и рекомендаций для быстрого усвоения теоретического материала и возможности его дальнейшего использования при выполнении домашних заданий, курсовых и дипломных проектов, а также при решении конкретных практических задач.

Для студентов вузов, обучающихся по направлению подготовки «Информатика и вычислительная техника» специальности «Автоматизированные системы обработки информации и управления»

Различные главы книги будут интересны и полезны также аспирантам, научным сотрудникам, преподавателям, слушателям второго высшего образования и широкому кругу специалистов, которым в своей работе приходится решать задачи, связанные с обслуживанием и сопровождением средств вычислительной техники.

УДК 004(075.8)
ББК 22.18я73

ISBN 978-5-7038-3655-2

Оглавление

Предисловие

В современных условиях, в процессе создания, установки и эксплуатации сложных автоматизированных систем обработки информации и управления (АСОИиУ), слишком дорого приходится платить за принятые недостаточно обоснованно технические, организационные и управленческие решения. Это касается, в частности, выбора архитектуры системы, выбора оборудования и настройки его рабочих параметров на требуемый режим работы, определения так называемых узких мест вычислительной системы и способов их устранения в процессе промышленной эксплуатации системы, выбора варианта маршрута прокладки кабеля, а также выбора варианта обслуживания и дальнейшего развития системы.

Современные специалисты: инженеры системотехники, инженеры по эксплуатации, администраторы системы, должны использовать в практической деятельности математический аппарат для обоснованного выбора наилучшего варианта решения проблемы, возникшей при эксплуатации системы, с целью ее оперативного разрешения и корректного выбора дальнейшего направления развития АСОИиУ..

Сокращение времени реакции системы на запрос пользователя, увеличение пропускной способности системы и среднего времени ее безотказной работы – вот те основные показатели функционирования АСОИиУ, построенной на основе локальных сетей, к достижению которых должен стремиться любой специалист, участвующий в обслуживании и сопровождении системы.

Цель учебного пособия состоит в содействии формированию у студентов базовых знаний, умений и навыков в области эксплуатации современных автоматизированных систем обработки информации и управления, построенных на базе локальных сетей, а также формированию у студентов устойчивой мотивации к анализу научно-технической информации и дальнейшему совершенствованию своих знаний.

Книга посвящена изложению основных понятий, методов, подходов, нормативных и руководящих документов, необходимых обслуживающему персоналу при проведении работ по эксплуатации автоматизированных систем обработки информации и управления, построенных на основе современных ЛВС семейства Ethernet. Эти работы включают выбор и установку оборудования и программных средств, настройку его рабочих параметров, проведение регламентных и профилактических мероприятий, а также сбор статистических данных о работе системы и ее отдельных компонент с целью определения и устранения узких мест, выработке рекомендаций по ее дальнейшему развитию и совершенствованию.

Преподавательский опыт автора показал, что теоретический материал прочно усваивается студентами только при решении задач, поэтому пособие имеет практическую направленность. Большинство разделов учебного пособия содержат примеры, помогающие в усвоении теоретического материала.

Материал, изложенный в пособии, может быть использован студентами при выполнении домашних заданий, курсовых и дипломных проектов, а также при выполнении научно-исследовательских работ.

Второе издание учебного пособия, по сравнению с первым «Основы эксплуатации автоматизированных систем обработки информации и управления. Краткий курс», претерпело существенные изменения. Учебное пособие разбито на два тома: том 1 – «Техническое обслуживание АСОИиУ» и том 2 – «Администрирование и развитие АСОИиУ». Перечислим основные изменения в томе «Администрирование и развитие АСОИиУ»:

- включены новые разделы, такие как «Конфигурирование технических средств АСОИиУ», «Администрирование СУБД Oracle», «Правовое обеспечение и стандартизация в сфере защиты информации», «Выбор вариантов развития АСОИиУ на основе аналитических методов», «Выбор вариантов развития АСОИиУ на основе экспертных методов», «Выбор вариантов развития АСОИиУ на основе методов теории массового обслуживания», «Обеспечение информационной безопасности», «Оценка рисков информационной безопасности»;
- более детально рассмотрены вопросы «Организация информационной безопасности АСОИиУ» и «Организация многоуровневой защиты информации в АСОИиУ»
- приведены модели анализа основных систем массового обслуживания и основные термины в области администрирования и развития АСОИиУ.

Учебное пособие состоит из семи глав и четырех приложений.

В первой главе рассмотрены основные направления деятельности администратора системы, задачи и средства, которые он использует в своей работе. Рассмотрены вопросы касающиеся адресации сетей и узлов АСОИиУ, а также конфигурирования технических средств АСОИиУ, на примере коммутаторов, для обеспечения их эффективной работы под управлением современного программного обеспечения.

Вторая глава посвящена основным направлениям администрирования сетевых операционных систем (ОС) Windows и Unix. Приведены рекомендации по настройке рабочих параметров сетевых ОС с целью увеличения их производительности и сбора статистических данных, необходимых для оперативного поиска и устранения «узких мест».

В третьей главе рассмотрены особенности администрирования наиболее широко используемых промышленных систем управления базами банных (СУБД) SQL Server и Oracle. Даны практические рекомендации по настройке рабочих параметров этих СУБД с целью увеличения производительности их работы и эффективности функционирования автоматизированной системы в целом..

Четвертая глава посвящена организации защиты информации в АСОИиУ. Рассмотрены вопросы, касающиеся стандартизации в сфере информационной безопасности, правового обеспечения защиты информации и оценки рисков информационной безопасности. Даны рекомендации администратору системы по формированию парольной системы защиты сервера. Особое внимание уделено вопросам организации многоуровневой защиты информации и формированию эффективной политики безопасности.

В пятой главе рассмотрены аналитические методы выбора вариантов развития действующих систем, в частности: метод сбалансированного критерия для выбора перспективного направления развития АСОИиУ, метод дерева целей для выбора стратегического плана развития АСОИиУ, метод анализа иерархий для принятия организационно-управленческих решений при модернизации АСОИиУ.

Шестая глава посвящена выбору вариантов развития АСОИиУ на основе экспертных методов. Показана возможность и целесообразность использования метода Дельфи и метода экспертных оценок для принятия организационно-управленческих решений при модернизации АСОИиУ.

В седьмой главе рассмотрены вопросы применения методов теории массового обслуживания для проведения сравнительной оценки альтернативных вариантов модернизации аппаратно-программных средств и организационных структур АСОИиУ.
В приложениях 1-4 рассмотрены вопросы обеспечения информационной безопасности АСОИиУ, методы оценки рисков информационной безопасности, приведены формулы для оценки характеристик функционирования систем массового обслуживания, моделирующих работу компонент АСОИиУ., а также приведены основные термины в области администрирования и развития АСОИиУ..

Пособие предназначено для студентов вузов, обучающихся по направлению подготовки “ Информатика и вычислительна техника” специальности “Автоматизированные системы обработки информации и управления”. Различные части пособия будут интересны и полезны аспирантам, научным сотрудникам, преподавателям, слушателям второго высшего образования и широкому кругу специалистов, которым в своей работе приходится решать проблемы, связанные с обслуживанием и сопровождением АСОИиУ.

Автор выражает благодарность рецензентам пособия за их огромный труд, замечания и полезные советы, которые они высказали в процессе его детального изучения.

Автор считает приятным долгом выразить благодарность своим коллегам: доценту Спиридонову С.Б., доценту Семкину П.С., к.т.н. доценту Ревункову Г.И., д.т.н., профессору Григорьеву Ю.А. и Постникову М.Е. за постоянные творческие дискуссии.

Особую благодарность автор выражает научному редактору Козлову С.В. (MCSE, MCITP, CCNP, MCT), д.т.н., профессору кафедры СМ-10 Жилейкину М.М. и заведующему кафедрой ИУ-5 д.т.н., профессору Черненькому В.М. за помощь и поддержку.

СПИСОК СОКРАЩЕНИЙ

АИС- автоматизированная информационная система

Глава 1 Основные направления деятельности администратора

1.1 Задачи и средства администратора системы

Администратор системы (системный администратор) — это один высококвалифицированный специалист или группа людей, которые вводят в действие, а затем эксплуатируют АСОИиУ предприятия. Администратор системы выполняет широкий спектр функций, в состав которых входят:

- установка и сопровождение аппаратно-программных средств системы;
- взаимодействие с поставщиками аппаратно-программных средств;
- настройка рабочих параметров и конфигурирование аппаратно-программных средств;
- консультирование обслуживающего персонала и пользователей;
- сбор статистики и управление работой системы для увеличения ее производительности и отказоустойчивости;
- диагностика работы системы для своевременного устранения возможных неполадок и сбоев в ее работе;
- поиск и устранение ошибок в работе аппаратно-программных средств;
- контроль, диагностика и управление параметрами электропитания системы;
- планирование развития системы и внедрения новых сервисов для совершенствования работы системы и удовлетворения постоянно растущих потребностей пользователей.

Выделяют следующие основные направления деятельности администратора системы:

- администрирование сетевой операционной системы (ОС) и сервера баз данных;
- администрирование процессов взаимодействия системы с оператором связи сети Интернет;
- администрирование процессов управления конфигурацией и мониторинга производительности;
- администрирование процессов обеспечения информационной безопасности;
- администрирование процессов эксплуатации и сопровождения системы, включающих проведение регламентных работ, архивацию и резервирование информации, диагностику системы, поиск и устранение неисправностей;

- администрирование процессов развития системы, включающих поиск и устранение узких мест, модернизацию и совершенствование организации вычислительных работ.

Рассмотрим основные направления деятельности администратора системы более подробно.

Администрирование сетевой ОС и сервера баз данных включает следующие работы:

- установку и настройку рабочих параметров сетевой ОС и сервера баз данных;
- установку и настройку рабочих параметров клиентского программного обеспечения (ПО) для работы пользователей в системе;
- создание списка пользователей и групп пользователей, установку режима их работы;
- создание сценариев регистрации для организации эффективной работы пользователей системы;
- обеспечение отказоустойчивой работы сервера системы благодаря использованию средств резервирования и дублирования;
- организацию вывода информации на печать на базе сервера печати;
- установку и настройку рабочих параметров системы управления базой данных (СУБД);
- создание концептуальной, логической и физической структуры базы данных, а также ее тестирование;
- установку и настройку рабочих параметров ПО, расширяющего функциональные возможности сетевой ОС, например веб-сервера и т. п.

Администрирование процессов взаимодействия системы с оператором связи сети Интернет включает следующие работы:

- выбор провайдера услуг связи:

– типа физического соединения с оператором;

– скорости передачи данных по физическому соединению;

– протокола передачи данных канального уровня, например PPP;

– IP-адресов для сети предприятия;

– оборудование для канала передачи данных и типа маршрутизатора;

- организацию взаимодействия системы с оператором связи сети Интернет по выбранному физическому каналу;
- определение вариантов IP-адресации и обеспечения безопасности передачи данных по физическому каналу;
- получение от провайдера адресного пространства на необходимое число IP-адресов;
- приобретение необходимого оборудования: модемов и маршрутизаторов;
- настройку режима передачи IP-трафика через маршрутизатор;
- получение у провайдера разрешения на выдачу серверу полномочий по обслуживанию системы доменных имен (Domain Name System–DNS) домена предприятия и запуск DNS-сервера;
- установку и конфигурирование сервера электронной почты;
- установку режима работы веб-телеконференций и веб-презентаций;;
- обеспечение доступа к системе предприятия удаленным пользователям;
- установку на рабочих станциях пользователей набора требуемого ПО.

Администрирование процессов управления конфигурацией и мониторинга производительности системы включает следующие работы:

- установку на специально выделенный компьютер ПО для управления работой сети. Примером такого ПО является, ПО Manage Wise или ПО HP OpenView. На узлы сети, по работе которых необходимо собирать статистику, следует установить ПО Agent;
- настройку рабочих параметров ПО на требуемый режим работы;
- установку и настройку рабочих параметров программ для оценки производительности и загрузки отдельных компонентов системы. К числу таких программ для ОС семейства Windows относят следующие:

– Performance monitor (монитор производительности) позволяющую получить полную информацию об организации вычислительного процесса на сервере в сети;

– Network Monitor (сетевой монитор), позволяющую получить полную и детальную информацию о работе сервера в сети, используя понятия объектов и счетчиков (объекты — процессор, оперативная память, задание, процесс, поток, физический диск и т. д;

счетчики — показатели, с помощью которых оценивают качество функционирования выбранного объекта, например процент использования, скорость работы, длина очереди и т. д.);

– Task Manager (диспетчер задач), дающую возможность получить обобщенную информацию об организации вычислительного процесса и выполнении прикладных программ (приложений), но не позволяющую отслеживать потоки информации.

Основное назначение мониторинга состоит в выявлении узких мест и их ликвидации с целью уменьшения времени реакции системы на запрос пользователя и увеличения пропускной способности системы.

Время реакции системы — это интервал времени между получением системой запроса от пользователя до момента возвращения ему результата ответа на его запрос.

Пропускная способность системы – это количество запросов пользователей, выполненных за единицу времени.

Эффективность системы – это свойство системы выполнять запросы пользователей в заданных условиях и с определенным качеством.

Основные подсистемы ПО для управления работой сети и их функции приведены в табл. 1.1

Таблица 1.1

Подсистемы ПО для управления работой сети и их функции

№ п/п	Подсистема ПО для управления работой сети	Основные функции подсистемы
1	Подсистема инвентаризации	1. Определение состава аппаратно-программных средств в узлах сети. 2. Проверка текущей аппаратно-программной конфигурации
2	Сбор статистических данных о работе сети	1. Определение времени работы узла сети. 2. Определение очередей к узлу сети. 3. Определение загрузки узла сети. 4. Определение узких мест сети
3	Диагностика сети и управление работой сети	1. Определение неисправностей в работе. 2. Ликвидация неисправностей. 3. Ликвидация узких мест сети
4	Обеспечение безопасности работы сети и конфиденциальности информации, хранящейся на сервере	1. Регистрация всех подключений пользователей к серверу. 2. Регистрация всех обращений пользователей к каталогам и файлам. 3. Регистрация входа пользователей в сеть и выхода из сети. 4. Ведение журнала учета по действиям пользователей и по работе узлов сети

Администрирование процессов обеспечения информационной безопасности включает следующие работы:

- соблюдение государственных стандартов и нормативов в сфере обеспечения информационной безопасности: ГОСТ 28147–89; ГОСТ Р 34.10–

04; ГОСТ Р 34.11–94; ГОСТ 29.339–92; ГОСТ Р 50752–95; ГОСТ РВ 50170–92; ГОСТ Р 50600–93; ГОСТ Р 50739–95; ГОСТ Р50922–96;

- установку, настройку рабочих параметров и регулярное использование комплекса программ, обеспечивающих защиту информации в системе от несанкционированного доступа, компьютерных вирусов, спама, а также от вредоносных программ. К числу программ защиты информации, не входящих в комплект поставки Windows, относят:

– Mc-Afee SpamKiler, работающую в фоновом режиме и позволяющую защитить компьютер от спама;

– Ad-Aware, осуществляющую защиту компьютера от вредоносных программ, в частности программ типа SpyWare и различных видов вирусов;

– Spybat Search & Destroy, позволяющую обнаружить и удалить различного вида вредоносные программы.

Встроенная в ОС Windows 7 программа «Защитник Windows» предназначена для защиты системы от посторонних вторжений, в частности от программ категории SpyWare. Она своевременно распознает опасность и выдает пользователю соответствующие сообщения, входит в комплект поставки сетевой ОС и инсталлируется автоматически с установкой ОС. Чтобы запустить программу, необходимо набрать в строке поиска меню «Пуск» запрос «Защитник Windows». В результате в верхней части меню появится команда для запуска. При ее активизации на экране монитора открывается окно программы.

Разработчики сетевых ОС постоянно выпускают обновления, которые в большинстве своем предназначены для решения следующих задач:

- улучшения функциональных возможностей сетевой ОС;
- устранения ошибок в работе сетевой ОС;
- повышения надежности сетевой ОС;
- увеличения уровня безопасности сетевой ОС от внешних угроз;
- упрощения процесса администрирования сетевой ОС.

Администрирование процессов эксплуатации и сопровождения системы включает следующие работы:

- диагностику системы, поиск и устранение неисправностей. Рекомендуется проводить диагностику в следующем порядке:

– собрать полную и исчерпывающую информацию об ошибке;

– разработать гипотезы по изоляции ошибок и ранжировать эти гипотезы по вероятности их весомости;

– проверить все гипотезы по очереди и провести документирование проблемы и способа ее решения;

- составление и постоянное пополнение каталога типовых неисправностей и способов их устранения. Например, диагностика ошибок сети Ethernet позволила установить, что причиной наличия пакета размером менее 64 байт

является неисправная сетевая плата, а причиной наличия пакета размером более 1 518 байт -– неисправность активного оборудования;

- архивацию информации, расположенной на дисках сервера и рабочих станциях пользователей;
- увеличение производительности системы за счет сокращения широковещательного трафика, настройки протоколов маршрутизации, снижения уровня электромагнитных помех;
- проведение ежедневных, еженедельных, ежемесячных регламентных работ, а также периодических и календарных работ.

Администрирование процессов развития системы включает следующие работы:

- проведение мониторинга компонентов системы с использованием теории планирования и организации экспериментальных исследований;
- анализ результатов мониторинга с целью определения узких мест системы;
- разработку мероприятий, направленных на устранение узких мест системы, для уменьшения времени реакции системы на запрос пользователя и увеличения пропускной способности системы;
- совершенствование организационной структуры системы;
- разработку комплексного плана перспективного развития системы и мероприятий, направленных на модернизацию и реорганизацию системы и ее отдельных компонентов.

1.2 Адресация сетей и узлов АСОИиУ

Современные АСОИиУ часто являются распределенными и объединяют в единую систему центральное отделение организации с ее филиалами и офисами, расположенными на значительном расстоянии друг от друга. Для передачи информации между отдельными АСОИиУ и соединения их в единую систему, как правило, используют стек протоколов TCP/IP (Transmission Control Protocol /Internet Protocol)., т.е. протокол управления передачей/межсетевой протокол. TCP действует на транспортном уровне, а IP на сетевом уровне семиуровневой модели взаимодействия открытых систем.. Стек протоколов TCP/IP является одним из самых распространенных стеков транспортных протоколов вычислительных сетей, поскольку объединяет компьютеры в сети Internet, а также широко используется в корпоративных и территориально-распределенных сетях, которые непосредственно не являются частями сети Internet.

При использовании стека протоколов TCP/IP основным способом связи для передачи информации между узлами АСОИиУ является IP-адресация, которая отличается большой

гибкостью и возможностью быстрого и простого способа включения отдельных узлов в сеть. При этом каждый узел такой сети имеет IP-адрес Узлами сети могут быть рабочие станции пользователей, серверы, маршрутизаторы и т. д.

IP-адрес узла характеризуется следующими особенностями:

- является уникальным и определяет местонахождение узла в распределенной сети;
- имеет стандартную длину 32 бита (IP v4);
- состоит из четырех восьмибитовых полей, называемых октетами;
- каждый октет представляет собой десятичное число в диапазоне от 0 до 255;
- при записи октеты отделяются друг от друга точками, что очень удобно для восприятия, например: 192.168.10.25.

При работе с IP-адресами необходимо знать правило преобразования двоичного формата IP-адреса в десятичный формат и наоборот (см. табл. 1.2)..

Таблица 1.2

Двоичный и десятичный форматы IP - адреса

Номер бита k	8	7	6	5	4	3	2	1
Значение бита двоичное	1	1	1	1	1	1	1	1
Значение бита десятичное 2^{k-1}	128	64	32	16	8	4	2	1

Согласно табл. 1.2:

- октету двоичного формата 00000111 соответствует октет десятичного формата 7, так как $2^2 + 2 + 2^0 = 7$;
- октету двоичного формата 01100001 соответствует октет десятичного формата 97, так как $2^6 + 2^5 + 2^0 = 97$;
- октету двоичного формата 11100110 соответствует октет десятичного формата 230, так как $2^7 + 2^6 + 2^5 + 2^2 + 2 = 230$.

Любой IP-адрес содержит четыре октета и состоит из двух частей: адреса сети и адреса узла в этой сети. В зависимости от того, какая часть IP-адреса отводится под адрес сети, а какая под адрес узла сети, различают пять классов IP-адресов: класс *A, B, C, D, E*. Принадлежность IP-адреса к тому или иному классу определяется значением старших бит первого октета этого IP-адреса.

Рассмотрим, как распределяются поля в IP-адресах разных классов.

IP-адреса класса *A*:

- назначаются узлам очень большой по размеру сети;
- старший бит в первом октете IP-адреса этого класса всегда равен нулю;

- семь бит первого октета, кроме старшего бита, представляют адрес сети;
- все 24 бита, входящие в состав второго, третьего и четвертого октетов, представляют адрес узла сети;
- адреса сетей этого класса находятся в диапазоне 1…126.

IP-адреса класса *B*:

- назначаются узлам большой и средней по размеру сети;
- два старших бита первого октета IP-адреса этого класса всегда имеют двоичное значение 10;
- оставшиеся шесть бит первого октета и все восемь бит второго октета представляют адрес сети;
- все 16 бит, входящие в состав третьего и четвертого октетов, представляют адрес узла сети;
- адреса сетей этого класса находятся в диапазоне 128…191.

IP-адреса класса *C*:

- назначаются узлам небольшой по размеру сети;
- три старших бита первого октета IP-адреса этого класса всегда имеют двоичное значение 110;
- оставшиеся пять бит первого октета, восемь бит второго октета и восемь бит третьего октета, т. е. 21 бит, представляют адрес сети;
- восемь бит, входящие в состав четвертого октета, представляют адрес узла сети;
- адреса сетей этого класса находятся в диапазоне 192…223.

IP-адреса класса *D*:

- четыре старших бита первого октета IP-адреса этого класса всегда имеют двоичное значение 1110;
- используются для широковещательной адресной рассылки
- Microsoft поддерживает IP-адреса класса *D*;

IP-адреса класса *E*:

- четыре старших бита первого октета IP-адреса этого класса всегда имеют двоичное значение 1111;
- в настоящее время адреса этого класса не применяются

Сводная информация об используемых классах IP-адресов дана в табл. 1.3.

Таблица. 1.3

Информация о классах IP- адресов

Показатель сравнения	Классы IP-адресов		
	Класс *A*	Класс *B*	Класс *C*
Диапазон значений первого октета (диапазон адресов сетей)	1–126	128–191	192–223
Возможное количество сетей	126	16 384	2 097 152
Возможное количество узлов в сети	16 777 214	65 534	254

Примечание. В качестве IP-адреса сети не может быть использовано значение 127, поскольку оно зарезервировано для передачи широковещательной информации и проведения самотестирования.

Каждый узел, находящийся в сети, кроме IP-адреса должен иметь маску сети. Маска сети — это 32-разрядное значение, которое используют для выделения (или маскирования) из IP-адреса его составных частей: адреса сети и адреса узла. В маске сети для всех бит IP-адреса, которые соответствуют адресу сети, устанавливают значение, равное единице, а для тех бит, которые соответствуют адресу узла, устанавливают значение, равное нулю. Значения маски сети для IP-адресов приведены в табл. 1.4

Таблица 1.4

Значения маски сети для IP-адресов

IP-адрес	Описание адреса сети в составе IP-адреса	Маска сети
IP-адрес класса *A*	Адрес сети – первый октет	255.0.0.0
IP-адрес класса *B*	Адрес сети – первые два октета	255.255.0.0
IP-адрес класса *C*	Адрес сети – первые три октета	255.255.255.0

Пример 1.1. Для IP-адреса 155.108.10.100, который относится к классу *B*, определить маску сети, адрес сети и адрес узла.

Решение. 1. Поскольку для IP-адреса, который относится к классу *B*, адрес сети определяется значением первого и второго октетов, то маска сети, согласно табл. П5.3, имеет вид 255.255.0.0.

2. Адрес сети определяется значением первого и второго октетов IP-адреса, поэтому он имеет вид 155.108.0.0.

3. Адрес узла определяется значением третьего и четвертого октетов IP-адреса, поэтому он имеет вид 0.0.10.100.

Довольно часто на практике перед администратором системы стоит задача разбиения сети, работающей на базе IP-адресов класса C, на отдельные рабочие подсети для обеспечения в них требуемой производительности, отказоустойчивости и конфиденциальности обрабатываемой информации.

Рассмотрим этапы разбиения исходной сети на *n* отдельных подсетей.

1. На первом этапе определяем разрядность маски IP-адресов рабочих подсетей класса *C*. Для этого сначала определяем максимальное число b_{m} возможных подсетей, округляя требуемое количество b рабочих подсетей до ближайшего большего целого числа, кратного степени числа два, при этом число a является степенью кратности. Поэтому должно быть выполнено условие

$$b \le b_{\text{m}} = 2^a \qquad (1.1)$$

После преобразования выражения (П6.1) получаем

$$a \ge \lg b / \lg 2 \qquad (1.2)$$

Находим минимальное целое значение числа a, которое удовлетворяет выражению (1.2).

Разрядность M маски IP-адресов рабочих подсетей класса C с учетом того, что разрядность маски IP-адресов сетей класса C равна 24 битам, определяем из выражения

$$M = 24 + a \text{ бит.} \qquad (1.3)$$

2. На втором этапе определяем маску IP-адресов рабочих подсетей класса *C*. Известно, что a бит, которые вычислены по выражению (1.2) входят в состав старших разрядов четвертого октета маски IP-адресов рабочих подсетей класса *C*. Для перевода значений a бит из двоичной системы в десятичную и получения значения четвертого октета маски выделяемых рабочих подсетей в десятичном виде A4 используем выражение

$$A4 = \sum_{i=1}^{a} 2^{8-i}. \qquad (1.4)$$

Получаем маску IP-адресов рабочих подсетей класса *C*, имеющую вид 255.255.255.A4, где A4 соответствует десятичному значению, вычисленному по выражению (1.4).

3. На третьем этапе определяем диапазон допустимых значений IP-адресов в каждой рабочей подсети, используя следующие правила:

- IP-адрес первой подсети должен совпадать с IP-адресом исходной сети;
- шаг h IP-адресов рабочих подсетей должен соответствовать значению последнего установленного бита в четвертом октете маски подсети, т. е. числу два в степени $8-a$. Поэтому имеем

$$h = 2^{8-a}; \qquad (1.5)$$

- первое значение диапазона допустимых значений IP-адресов узлов подсети должно быть на единицу больше адреса этой подсети;

- последнее значение диапазона допустимых значений IP-адресов узлов подсети должно быть на две единицы меньше IP-адреса следующей подсети;
- последнее значение диапазона допустимых значений IP-адресов узлов подсети должно быть на одну единицу меньше IP-адреса, который отводится для передачи широковещательной информации в этой подсети.

Пример 1.2. Дан IP-адрес 202.185.10.0 сети класса *C*. Необходимо разбить данную сеть на пять одинаковых по размеру рабочих подсетей и для каждой из них указать диапазон допустимых IP-адресов.

Число рабочих подсетей исходной сети $b = 5$

Решение. 1. Последовательно используя выражения (1.1), (1.2) и (1.3), находим:

- максимальное количество возможных подсетей $b_{\text{m}} = 8$
- количество бит старших разрядов четвертого октета IP-адреса, которые входят в состав маски IP-адресов рабочих подсетей класса *C* $a = 3$;
- разрядность маски IP-адресов рабочих подсетей класса *C* $M = 24 + 3 = 27$ бит.

2. Используя выражение (1.4), находим в десятичном виде значение четвертого октета маски выделяемых рабочих подсетей:

$$A4 = \sum_{i=1}^{3} 2^{8-i} = 2^7 + 2^6 + 2^5 = 128 + 64 + 32 = 224.$$

Получаем значение маски IP-адресов рабочих подсетей класса *C*, имеющее следующий вид: 255.255.255.224.

3. Определяем диапазон допустимых IP-адресов в каждой рабочей подсети, используя приведенные ранее правила, которые описаны при выполнении этапа 3. При этом шаг *h* IP-адресов рабочих подсетей исходной сети вычисляем по выражению (1.5) и получаем

$$h = 2^{8-a} = 2^5 = 32.$$

Все остальные результаты, полученные на основании использования правил определения диапазона допустимых IP-адресов в каждой рабочей подсети, приведены в табл. 1.5

Таблица 1.5

Характеристики рабочих подсетей

Номер подсети	Допустимые IP-адреса	IP-адрес рабочей подсети	IP-адреса узлов рабочей подсети
Рабочие подсети исходной сети			
1	от 202.185.10.1 до 202.185.10.30	202.185.10.0	от 202.185.10.1 до 202.185.10.30
2	от 202.185.10.33 до 202.185.10.62	202.185.10.32	от 202.185.10.33 до 202.185.10.62
3	от 202.185.10.65 до 202.185.10.94	202.185.10.64	от 202.185.10.65 до 202.185.10.94
4	от 202.185.10.97 до 202.185.10.126	202.185.10.96	от 202.185.10.97 до 202.185.10.126
5	от 202.185.10.129 до 202.185.10.158	202.185.10.128	от 202.185.10.129 до 202.185.10.158
Возможные дополнительные подсети			
6	от 202.185.10.161 до 202.185.10.190	202.185.10.160	от 202.185.10.161 до 202.185.10.190
7	от 202.185.10.193 до 202.185.10.222	202.185.10.192	от 202.185.10.193 до 202.185.10.222
8	от 202.185.10.225 до 202.185.10.255	202.185.10.224	от 202.185.10.225 до 202.185.10.255

1.3 Конфигурирование технических средств АСОИиУ

Конфигурирование технических средств АСОИиУ, которое выполняет администратор системы, рассмотрим на примере настройки рабочих параметров коммутаторов.

Управляемые коммутаторы обычно оснащены консольным портом, имеющим разъем Rj-45. С помощью консольного кабеля, входящего в комплект поставки, коммутатор подключают к порту Rj-45 того компьютера, с которого будут производить настройку параметров коммутатора.

Поясним принципы конфигурирования коммутаторов и настройку их рабочих параметров на примере коммутатора DES-3528 фирмы D-Link.

Обычно для настройки конфигурации коммутатора используют команды командной строки, количество которых достаточно большое, при этом каждая команда может иметь свой набор параметров.

Для того, чтобы вывести на экран список всех команд коммутатора и с ними ознакомится, следует набрать в командной строке знак вопроса «?» и нажать клавишу «Enter», а чтобы узнать возможные варианты синтаксиса какой-либо команды, например, команды «show switch» коммутатора DES 3528, следует ввести в командной строке следующую последовательность символов: DES 3528 # show switch+ пробел «Enter».

Следует иметь в виду, что команды типа «show» являются самым удобным средством проверки состояния и параметров коммутатора, предоставляя администратору также информацию, требуемую для мониторинга и поиска неисправностей в работе коммутатора.

В табл. 1.6 приведены наиболее часто используемые команды типа «show».

Таблица 1.6

Команды вывода на экран монитора параметров коммутатора.

Команда типа «show»	Назначение команды
show config	Просмотр конфигурации коммутатора, сохраненной в энергонезависимой памяти (NVRAM) или созданной в текущий момент
show device_status	Просмотр состояния внутреннего и внешнего питания коммутатора
show error ports	Просмотр статистики об ошибках для заданного диапазона портов
show fdb	Просмотр текущей таблицы коммутации
show firmware information	Просмотр информации о программном обеспечении коммутатора (прошивке)
show ipif	Просмотр информации о настройках IP-интерфейса на коммутаторе
show scheduling	Просмотр текущего расписания обработки пакетов, находящихся в очередях
show switch	Просмотр общей информации о коммутаторе

Коммутаторы допускают приоритетное обслуживание поступающих пакетов. Поскольку высокоприоритетные пакеты должны обрабатываться раньше низкоприоритетных, то в коммутаторы имеют несколько очередей приоритетов (до 8) на каждый порт. Поступающие в коммутатор пакеты помещаются в разные очереди обслуживания, в соответствии со своими приоритетами.

Для обработки пакетов, находящихся в очередях коммутатора, администратор может использовать любой из следующих двух механизмов обслуживания очередей:

- строгая очередь приоритетов (Strict Priority Queuing), когда пакеты, находящиеся в самой приоритетной очереди, начинают обслуживаться первыми и пока более приоритетная очередь не опустеет, пакеты из менее приоритетных очередей обслуживаться не будут;
- взвешенный циклический алгоритм (Weighted Round Robin - WRR), когда для каждой приоритетной очереди задается максимальное количество пакетов, которое может быть передано за один раз, и максимальное время ожидания, через которое очередь снова сможет передавать пакеты. Диапазон передаваемых пакетов от О до 255, а диапазон времени ожидания от 0 до 255 (увеличивается на 16 мс).

В табл. 1.7 приведены команды для настройки приоритетной обработки пакетов с помощью команд командной строки

Таблица 1.7

Команды для настройки приоритетной обработки пакетов в коммутаторе.

Команда	Параметр	Назначение
config 802.1p user_priority	<priority 0-7> <class_id 0-3>	Привязка входящего пакета, с заданным пользователем приоритетом 802. 1р, к очереди на коммутаторе
config scheduling	<class_id 0-3> max_packet <value 0-255> max_latency <value 0-255>	Настройка расписания обработки пакетов каждой приоритетной очереди
show 802. Ip user_priority		Просмотр текущей схемы привязки приоритетов очередям

Пример 1.3. Поместите пакеты, маркированные, согласно стандарта Ethernet 802.1p, с приоритетом 1 в очередь Q3 коммутатора DES-3528 фирмы D-Link.

Решение. DES-3528 config 802.lp user_priority 1 3
Command: config 802.1p user_priority 1 3
Success.

Пример 1.4. Создайте для очереди Q3, коммутатора DES-3528 фирмы D-Link,. расписание обработки поступающих в нее пакетов согласно алгоритму WRR, при этом максимальное количество передаваемых пакетов за один раз равно 100, а время ожидания повторной передачи – 150 мс.

Решение. DES- 3528# config scheduling 3 max_packet 100 max_latency 150
Command: config scheduling 3 max_packet 100 max_latency 150
Success.

Пример 1.5. Назначьте всем немаркированным пакетам, приходящим на любой из портов коммутатора DES-3528 фирмы D-Link,. приоритет 5.

Решение. DES-3528#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5
Success.

Помните, что все команды чувствительны к регистру, поэтому перед вводом команд удостоверьтесь в том, что регистр выбран правильно.

Настройка рабочих параметров коммутатора предусматривает последовательное выполнение следующих этапов:

Этап 1. Защита коммутатора от доступа неавторизованных пользователей.
Этап 2 Настройка IP-адреса коммутатора.
Этап 3. Настройка параметров портов коммутатора.
Этап 4. Сохранение текущей конфигурации коммутатора.
Этап 5. Перезагрузка коммутатора.
Этап 6. Просмотр текущей конфигурации коммутатора.

На первом этапе настройки коммутатора для защиты его от доступа неавторизованных пользователей следует создать учетные записи пользователей, количество которых должно быть не более 8. Для каждой учетной записи следует задать имя пользователя, пароль и один из следующих уровней привилегий:Admin, Operator, User.

Учетная запись пользователя с привилегией:

- Admin имеет наивысший уровень привилегий и максимальные права управления коммутатором;
- Operator имеет права управления коммутатором, включающие мониторинг сети, чтение системных параметров и параметров конфигураций;
- User имеет минимальные права, включающие только чтение

Длина имени пользователя должна быть от 1 до 15 символов, а длина пароля пользователя от 0 до 15 символов.
Для создания учетной записи пользователя используется команда «Create account» с параметрами «уровень привилегий» «имя пользователя»
После создания учетной записи следует ввести пароль «password»
Введенные символы пароля на экране монитора заменяются звездочками

После успешного создания учетной записи пользователя на экране монитора появится слово *Success (успешно)*

Пример 1.6. Создайте учетную запись с уровнем привилегий «admin» и именем пользователя «user5» на коммутаторе DES-3528:

Решение • 3528#create account admin user5
Command : create account admin user5
Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success

Для замены старого пароля пользователя на новый пароль следует использовать команду «config account» с параметром «имя пользователя». Далее приведен пример замены пароля для пользователя с именем «user5»

Пример 1.7. Замените пароль для пользователя с именем «user5»

Решение. DES-3528#config account user5
Command: config account user5
Enter a old password:****
Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success

Для удаления учетной записи пользователя следует использовать команду «delete account» с параметром «имя удаляемого пользователя».

Пример 1.8. Удалите созданную учетную запись пользователя с именем «user6».

Решение. DES-3528# delete account user6
Command: delete account user6
Success

На втором этапе коммутатору необходимо назначить IP- адрес сети, в которой планируется его использовать. Этот IP- адрес можно задать с помощью следующей команды с параметрами:

config ipif System ipaddress xxx.xxx.xxx.xxx/ yyy.yyy.yyy.yyy.

Где config ipif- команда задания IP- адреса коммутатора;
System – имя управляющего интерфейса коммутатора;.
ipaddress – параметр, определяющий начало IP- адреса;
xxx.xxx.xxx.xxx- IP адрес сети
yyy.yyy.yyy.yyy – маска подсети
Далее приведен пример использования этой команды
DES-3528#config ipif System ipaddress
192.168.100.240/255.255.255.0
Command: config ipif System ipaddress 192.168.100.240
Success.

На третьем этапе осуществляем настройку портов коммутатора на требуемый режим работы

Пример 1.9 Для первого, второго и третьего портов коммутатора DES-3528 следует произвести следующие настройки:

- установить скорость передачи равной 10 Мбит/с;
- установить дуплексный режим работы;
- обеспечить управление потоком;
- перевести порты в состояние «включено».

Решение. DES 3528# config ports 1-3 speed 10_full learning enable
state enable flow _control enable
Command : config ports 1-3 speed 10_full learning enable
state enable flow _control enable
Success

На четвертом этапе необходимо сохранить текущую конфигурацию коммутатора и записать ее в энергонезависимую память (памяти NV-RAM).

Для этого следует выполнить команду «»save» (записать), которая имеет следующий вид:

DES-3528#save
Command: save
Saving all settings to NV-RAM

Следует помнить, что рабочая конфигурация коммутатора всегда хранится в оперативной памяти (памяти типа SDRAM). При отключении питания коммутатора от сети, конфигурация коммутатора, хранимая в этой памяти, будет потеряна. Для того чтобы сохранить рабочую конфигурацию коммутатора ее необходимо записать в энергонезависимую память NV-RAM.

Никогда не сохраняйте настройки конфигурации коммутатора после создания пользователей, не проверив их. Обязательно войдите в систему с помощью каждой из созданных настроек. Помните, что в случае утраты сведений об имени пользователя и его пароле, разблокировать коммутатор можно только в сервисном центре компании D-Link!

На пятом этапе необходимо выполнить перезагрузку коммутатора, используя команду «reboot», которая имеет следующий вид:

DES-3528#reboot
Command: reboot
Are you sure you want to proceed with the system reboot? (y/n)
Please wait, the switch is rebooting...

Сброс настроек коммутатора и переход к заводским настройкам выполняется с помощью команды «reset» с ключевыми словами, которая имеет следующий вид: reset {[config | system]} {force_agree}

При этом возможны следующие варианты записи команды «reset»:

-

если в команде «reset» не будет указано никаких ключевых слов, то все параметры, за исключением IP-адреса, учетных записей пользователей и журнала историй, будут возвращены к заводским параметрам по умолчанию, например:

```
DES-3528 # reset
Command reset
Success
```

- если команда имеет вид «reset config», то на коммутаторе восстановятся все заводские настройки по умолчанию, включая IP-адрес, учетные записи пользователей и журнал историй, например:

```
DES-3528 # reset config
Command reset config
Success
```

- если команда имеет вид «reset system», то на коммутаторе восстановятся все заводские настройки по умолчанию в полном объеме, он сохранит их в энергонезависимой памяти и перезагрузится, например:

```
DES-3528 # reset system
Command reset system
Success
```

- если команда имеет вид «reset force_agree», то произойдет безусловное выполнение команды «reset». Не нужно вводить Y/N. На коммутаторе восстановятся все заводские настройки по умолчанию, исключая IP-адрес, учетные записи пользователей и журнал историй, например:

```
DES-3528 # reset force_agree
Command reset force_agree
Success
```

На шестом этапе необходимо выполнить просмотр конфигурации коммутатора. Получить информацию о коммутаторе, т.е. просмотреть его текущую конфигурацию, можно с помощью команды «show switch».Для коммутатора DES 3528 после запуска команды «show switch».можно получить следующую информацию:

DES-3528#show switch
Command: show switch
IP Address: 192.168.100.240
Sabnet Mask: 255.255.255.0
Default Gateway: 0.0.0.0
Firmware Version: Build 2.20.B028
Hardware Version: A1

Контрольные вопросы и задания к главе 1

1. Перечислите задачи, которые должен решать администратор системы.

2. Перечислите средства, используемые администратором системы.

3. Поясните назначение встроенной в ОС Windows 7 программы «Защитник Windows».
4. Поясните различие между следующими показателями работы АСОИиУ: время реакции, пропускная способность, эффективность работы.
5. Перечислите компоненты АСОИиУ, которым присваивают IP – адрес.
6. Перечислите этапы разбиения сети на отдельные подсети.
7. Поясните назначение маски IP- сети.
8. Поясните, как осуществляется приоритетное обслуживание пакетов, поступающих в коммутатор.
9. Перечислите привилегии для учетной записи пользователя.
10. В какой памяти хранится конфигурация коммутатора.

Литература к главе 1

Основная

Беленькая Н.М. Администрирование в информационных системах / Н.М. Беленькая, С.Т. Малиновский, И.В. Яковенко. М.: Горячая линия Телеком, 2011. 400 с.

Дополнительная

Кенин А.М. Самоучитель системного администратора / А.М. Кенин. СПб.: БХВ Петербург, 2008. 560 с.

Поляк-Брагинский А. Администрирование сети на примерах: пер. с англ. / А. Поляк-Брагинский. СПб.: БХВ Петербург, 2005. 320 с.

Глава 2 Основы администрирования сетевых операционных систем

2.1 Администрирование сетевых ОС семейства Windows

Сетевая ОС Microsoft Windows Server помогает администратору полностью контролировать инфраструктуру и аппаратные средства системы, обеспечивая доступность, управляемость, функциональность, гибкость, безопасность, надежность и устойчивость работы файлового сервера.

Сетевая ОС Microsoft Windows Server позволяет администратору:

- использовать эффективные средства группового администрирования;
- обнаруживать и устранять неполадки с помощью средств диагностики.

Мастер настройки файлового сервера позволяет администратору быстро устанавливать, добавлять и удалять роли сервера: сервер печати, сервер удаленного доступа, сервер доменных имен и т. д. Число ролей сервера, работающего под управлением ОС Microsoft Windows Server, неограниченно.

Важным моментом работы администратора является настройка политики безопасности системы, состоящей из набора взаимодействующих серверов, входящих в состав домена, или отдельных серверов и локальных компьютеров. Политика безопасности домена или одного сервера представляет собой сочетание всех параметров, регулирующих его безопасность и позволяющих администратору:

- обеспечивать санкционированный доступ пользователей к серверу;
- назначать ресурсы, которые может использовать каждый пользователь;
- управлять ведением журнала событий, т. е. включением или отключением записи действий пользователя или группы пользователей в журнал событий.

При изменении любого параметра безопасности, параметры безопасности обновляются каждые 90 мин на компьютере и/или файловом сервере и каждые 5 мин на контроллере домена. Кроме того, независимо от наличия изменений параметры обновляются каждые 16 ч. Для немедленного вступления изменений в силу в командной строке соответствующего файлового сервера следует набрать команду grupgrade.exe.

Для изменения локальной политики безопасности администратору следует выполнить команды «Пуск» — «Администрирование» — «Локальная политика безопасности». На экране монитора появится окно настройки рабочих параметров локальной политики безопасности. Используя информацию, приведенную в этом окне настройки, можно задать политику аудита, присвоить права пользователям, установить параметры безопасности файл-сервера.

Шаблон политики безопасности домена аналогичен шаблону локальной политики безопасности. Политика безопасности домена применяется ко всем файл-серверам в домене, а не только к одному локальному файл-серверу, на котором она установлена. Политику безопасности домена администратор настраивает с консоли файл-сервера домена с помощью команд «Пуск» — «Администрирование» — «Политика безопасности домена».

Политика ограничения программ позволяет администратору задавать программы, которые можно запускать на файл-сервере, и учетные записи пользователей, имеющих доступ к этим программам.

К достоинствам файловой системы новой технологии (New Technology File System-NTFS), используемой в операционных системах семейства Windows, можно отнести:

- надежность, поскольку ОС имеет механизм транзакций, при котором незавершенные файловые операции отменяются;
- гибкость, так как размер кластера администратор может изменять в широком диапазоне значений от 512 байт до 64 Кбайт;
- поддержку длинных имен файлов;
- обеспечение шифрования и прозрачного сжатия файлов;
- мощную модель безопасности, включающую до 13 атрибутов файлов.

Для ограничения доступа локальных и удаленных пользователей к каталогам (папкам) и файлам, расположенным на файловом сервере с ОС Windows Server, администратор устанавливает для пользователей разрешения.

Каждому файлу или папке администратор может назначить или отменить до семи основных типов разрешений (табл. 2.1).

Таблица 2.1

Типы разрешений, используемых в сетевых ОС семейства Windows

№	Тип разрешения	Описание
1	Full Control (полный доступ)	Обеспечивает полное управление папками и файлами, в том числе позволяет назначать разрешения
2	Modify (изменение)	Предоставляет все разрешения, кроме возможности передавать разрешения другим пользователям. Позволяет читать, удалять, изменять и перезаписывать файлы и папки
3	Read & Execute (чтение и выполнение)	Дает возможность читать разрешения и запускать программные файлы
4	List (Folders Only) (чтение содержимого папки)	Позволяет просматривать имена файлов и подпапок внутри папки
5	Read (чтение)	Обеспечивает просмотр, копирование, печать и переименование файлов, папок и объектов. Не позволяет запускать выполняемые программы, кроме файлов сценариев. Дает возможность считывать разрешения объектов, атрибуты объектов и расширенные атрибуты (например, бит Archive, EFS). Позволяет составлять списки файлов и подпапок папки
6	Write (запись)	Разрешает читать, создавать и перезаписывать файлы и папки
7	Special Permissions (особые разрешения)	Позволяет составлять комбинации из 14 более детальных разрешений, которые не приведены в этой таблице

При большом числе пользователей администратору следует разделить их на локальные группы, которым предоставляются одинаковые и определенные права доступа.

Для упрощения процесса администрирования системы набор разрешений на доступ к определенным папкам и файлам администратору следует назначать отдельно для каждой группы пользователей, а в дальнейшем просто добавлять в эту группу (или исключать из нее) новых пользователей без изменения набора разрешений.

В ОС Windows с файловой системой FS для более детального управления разрешениями пользователей и групп, кроме основных разрешений используют и специальные разрешения. В табл. 2.2 приведены основные разрешения и соответствующие им специальные разрешения. В табл. 2.3 приведена комбинационная связь основных и специальных разрешений

Таблица 2.2

Основные и специальные разрешения, используемые в ОС Windows 8

№	Основное разрешение	Специальное разрешение
1	Read (чтение)	List folder / read data (содержание папки / чтение данных)
		Read attributes (чтение атрибутов)
		Read extended attributes (чтение дополнительных атрибутов)
		Read permissions (чтение разрешений)
2	Read & Execute (чтение и выполнение)	List folder / read data (содержание папки / чтение данных)
		Read attributes (чтение атрибутов)
		Read extended attributes (чтение дополнительных атрибутов)
		Read permissions (чтение разрешений)
		Traverse folder / execute file (траверс папок / выполнение файлов)
3	Write (запись)	Create files / write data (создание файлов / запись данных)
		Create folder / append data (создание папок / дозапись данных)
		Write attributes (запись атрибутов)
		Write extended attributes (запись дополнительных атрибутов)
4	Modify (изменение)	все специальные разрешения для (чтение)
		все специальные разрешения для (запись)
		Delete (удаление)
5	Full Control (полный доступ)	все ранее перечисленные специальные разрешения
		Change permission (смена разрешений)
		Delete subfolders and files (удаление подпапок и файлов)
		Take ownership (смена владельца)

Таблица 2.3

Комбинационная связь основных и специальных разрешений, используемых в ОС Windows

Специальные разрешения	Основные разрешения				
	Full control	Modify	Read & Execute	Read	Write
List folder / read data (содержание папки / чтение данных)	*	*	*	*	
Read attributes (чтение атрибутов)	*	*	*	*	
Read extended attributes (чтение дополнительных атрибутов)	*	*	*	*	
Read permissions (чтение разрешений)	*	*	*	*	*
Traverse folder / execute file (траверс папок / выполнение файлов)	*	*	*		
Create files / write data (создание файлов / запись данных)	*	*			*
Create folder / append data (создание папок / дозапись данных)	*	*			*
Write attributes (запись атрибутов)	*	*			*
Write extended attributes (запись дополнительных атрибутов)	*	*			*
Delete (удаление)	*	*			
Change permission (смена разрешений)	*				
Delete subfolders and files (удаление подпапок и файлов)	*				
Take ownership (смена владельца)	*				

Примечание. Основные разрешения Read & Execute (чтение и выполнение) и List FolderContents (список содержимого папки) ОС Windows, имеют одинаковый набор входящих в них специальных разрешений, поэтому разрешение List FolderContents не приведено в табл. 2.2 и 2.3. Однако, следует иметь в виду, что у этих разрешений есть некоторое различие:

- разрешение Read & Execute наследуется всеми папками и файлами, вложенными в рассматриваемую папку;
- разрешение List Folder Contents наследуется только папками, вложенными в рассматриваемую папку, но не наследуется файлами этой папки и файлами, расположенными во вложенных папках.

Наследование разрешений означает, что на папки и файлы переносятся разрешения, назначенные родительской папке, при условии, что наследование для родительской папки ранее было разрешено. По умолчанию, разрешения папки наследуются всеми папками и файлами, находящимися в ней. Если администратор системы предоставляет пользователю доступ к папке с помощью какого-либо разрешения, то он тем самым автоматически открывает этому пользователю доступ ко всем папкам и файлам, которые находятся в этой папке.

Пользователь получает разрешения к папке и файлам индивидуально, либо в результате его принадлежности к одной или нескольким группам.

Назначая пользователям или членам группы специальное разрешение «Take ownership» (смена владельца), администратор системы позволяет им в дальнейшем стать владельцами соответствующих папок и/или файлов.

Если пользователи или группы уже созданы и находятся в списке на вкладке «безопасность», то их разрешения можно изменить. Для этого следует нажать кнопку

«изменить» и затем установить или снять флажки требуемых разрешений в списке «разрешения». Чтобы добавить разрешение на выполнение определенного действия, нужно установить его флажок в столбце «разрешить», а чтобы отменить разрешение – снять его флажок. Чтобы запретить выполнение определенного действия, нужно установить его флажок в столбце «запретить». Запрещенные полномочия имеют приоритет над разрешенными.

Администратору системы следует соблюдать следующие правила назначения пользователям разрешений для работы с папками и файлами:

- фактические разрешения, которые имеет пользователь, – это наиболее разрешающая комбинация его индивидуальных разрешений и разрешений всех групп, в которые он входит;
- отсутствие любых разрешений у пользователя или группы, в которую он входит, отменяет все разрешения для данного пользователя;
- разрешения на файл превалируют над разрешениями папки, в которой находится данный файл;
- для выполнения копирования папок и/или файлов в пределах логического диска сервера пользователь должен иметь разрешение «Write» на папку, в которую копируемая информация будет размещена;
- для выполнения перемещения папок и/или файлов в пределах логического диска сервера пользователь должен иметь разрешение «Write» на папку, в которую перемещаемая информация будет размещена и разрешение «Modify» на папку, в которой эта информация была первоначально размещена.

Рассмотрим примеры, поясняющие особенности назначения пользователю разрешений при работе с папками и файлами.

Пример 2.1. Пользователь «user1» имеет разрешение «Read» на файл «a.doc». Он является членом двух групп «gr1» и «gr2», для которых на этот файл установлены соответственно следующие разрешения «Modify» и «Write». Поясните, какое фактическое разрешение имеет пользователь «user1» на файл «a.doc».

Решение. Поскольку пользователь «user1» и группы, в которые он входит, имеют определенные разрешения для работы с файлом «a.doc», то фактическое разрешение пользователя «user1» на файл «a.doc» будет «Modify» , как наиболее разрешающее.

Пример 2.2. Пользователь «user1» имеет разрешение «Read» на файл «c.doc». Он является членом двух групп «gr1» и «gr2». Для членов группы «gr1» на файл «c.doc». установлено разрешение «Modify», а члены группы «gr2» на этот файл не имеют никаких разрешений. Поясните, какое фактическое разрешение имеет пользователь «user1» на файл «c.doc».

Решение. Поскольку пользователь «user1» входит в состав группы «gr2», члены которой не имеют никаких разрешений на файл «c.doc», то пользователь «user1» также не имеет никаких разрешений на этот файл и доступ к файлу «c.doc» ему будет запрещен.

Пример 2.3. Пользователь «user1» имеет разрешение «Read» на папку « k1» и разрешение «Write» на файл «e.doc», который находится в этой папке. Поясните, какие действия с файлом «e.doc» и другими файлами, находящимися в папке « k1», может производить пользователь «user1».

Решение. Поскольку пользователь «user1» имеет разрешение «Write» на файл «e.doc», то он может производить запись информации в это файл, а поскольку он также имеет разрешение «Read» на папку « k1», то он может читать содержимое других файлов этой папки, но не может их изменять или создавать в этой папке новые файлы.

При работе в сети отдельные папки поступают в общее пользование и являются общим ресурсом для многих пользователей. В этом случае отдельным пользователям и группам пользователей администратор системы присваивает также разрешения доступа к общему ресурсу. Совместное использование администратором сети общих разрешений и разрешений доступа к общему ресурсу обеспечивает наивысшую степень защиты информации на сервере. Фактическим разрешением доступа пользователей к общему ресурсу, при наличии общих разрешений и разрешений общего доступа, является наименьшее из этих разрешение, которое обеспечивает усиление защиты информации.

Пример 2.4. Для общей папки «k0» на сервере установлено общее разрешение «Read» и разрешение доступа по сети «Full Control». Определите фактическое разрешение для доступа пользователей к этой общей папке.

Решение. Фактически пользователи будут иметь к общей папке «k0» разрешение «Read», как наименьшее из двух установленных разрешений.

Пример 2.5. Пользователь «user1» к общей папке «k0», размещенной на удаленном компьютере, имеет разрешение доступа «Read» и разрешения «Full Control» на файл «a.doc» и «Read» на файл «c.doc», находящиеся в этой общей папке. Определите, какие фактические разрешения имеет пользователь «user1» на файлы «a.doc» и «c.doc».

Решение. Пользователь «user1» к файлам «a.doc» и «c.doc», размещенным в общей папке «k0» на удаленном компьютере, имеет разрешение «Read», как наименьшее из всех установленных разрешений.

Сетевые ОС семейства Windows имеют системный монитор, который содержит много объектов и счетчиков, позволяющих получать статистические данные о работе основных ресурсов файл-сервера: процессора, памяти, физических дисков и т. д. Перечислим наиболее часто используемые администратором сети счетчики.

Счетчики объекта «Процессор»:

- процент времени С1 — процент времени, в течение которого процессор простаивает;
- процент времени прерываний — процент времени, которое процессор тратит на получение и обслуживание аппаратных прерываний;
- процент загруженности процессора — процент времени, которое процессор тратит на обработку всех потоков команд.

Счетчики объекта «Физический диск»:

- процент активности диска — процент времени, затраченного выбранным дисковым устройством на обработку запросов на чтение и запись данных;
- число обращений записи на диск в секунду — частота выполнения операций записи на этот диск;
- число обращений чтения с диска в секунду — частота выполнения операций чтения с этого диска;
- число обращений к диску в секунду — частота выполнения операций чтения и записи на этот диск;
- скорость записи на диск (байт/с) — скорость передачи данных на этот диск при выполнении операций записи;
- скорость чтения с диска (байт/с) — скорость передачи данных с этого диска при выполнении операций чтения;
- скорость обмена с диском (байт/с) — скорость обмена данными с этим диском при выполнении операций чтения или записи;
- среднее время записи на диск (с) — среднее время, затрачиваемое на одну операцию записи данных на диск;
- среднее время чтения с диска (с) — среднее время, затрачиваемое на одну операцию чтения данных с диска;
- среднее время обращения к диску (с) — среднее время, затрачиваемое на одну операцию обмена данными с диском;
- средний размер одной записи на диск (байт) — среднее число байтов данных, переданных на диск при выполнении операций записи;
- средний размер одного чтения с диска (байт) — среднее число байтов данных, полученных с диска при выполнении операций чтения;
- средний размер одного обмена с диском (байт) — среднее число байтов данных, переданных при выполнении операций чтения или записи;

• средняя длина очереди записи на диск — среднее число запросов на запись, которые были поставлены в очередь для соответствующего диска в течение интервала измерения;

• средняя длина очереди чтения с диска — среднее число запросов на чтение, которые были поставлены в очередь для соответствующего диска в течение интервала измерения;

• средняя длина очереди диска — среднее общее число запросов на чтение и на запись, которые были поставлены в очередь для соответствующего диска в течение интервала измерения;

• текущая длина очереди диска — число невыполненных запросов к диску во время сбора сведений о его загруженности.

Счетчики объекта «Система»:

• операции чтения файлов в секунду — среднее число всех операций чтения файловой системы данного компьютера;

• системные вызовы в секунду — частота обращений к процедурам системных служб ОС;

• потоки — число потоков в компьютере в момент сбора информации;

• процессы — число процессов в компьютере в момент сбора информации.

Сетевые ОС семейства Windows имеют также компонент «Журналы и оповещения о производительности», позволяющий собирать данные о производительности компьютеров и их компонентов в автоматическом режиме. Сведения из этих журналов и данные о состоянии счетчиков можно получить на экране файл-сервера в виде диаграмм или гистограмм. Ведение журналов является наиболее распространенным способом наблюдения за работой сети. Это наблюдение администратору следует осуществлять с интервалом не менее 15 мин, чтобы не загружать систему фоновым потоком статистики.

При наблюдении за большим числом объектов и счетчиков обычно записываются большие объемы данных, занимающих дисковое пространство

и существенно снижающих производительность сети. Администратор должен определить оптимальное соотношение между числом наблюдаемых объектов и частотой обновления данных, чтобы размер файла журнала был не слишком большим, но в то же время давал объективную оценку качества работы системы.

Наблюдения за работой системы позволяют администратору обнаружить избыточный спрос на определенные ресурсы, который может привести к возникновению узких мест в работе системы.

Ниже перечислены основные причины возникновения узких мест в работе системы под управлением ОС семейства Windows и даны рекомендации по их устранению.

1. Если загрузка ресурса более 75 %, требуется нарастить его мощность или заменить на более производительный.

2. При неравномерной загрузке идентичных ресурсов (например, дисков сервера) необходимо перераспределить размещенную на них информацию.

3. Если ресурс неисправен или дает сбои, требуется его заменить.

4. В случае использования ресурса медленной программой в монопольном режиме необходимо заменить эту программу на более быструю.

5. Для обеспечения эффективного функционирования ресурса системы необходима корректная настройка его рабочих параметров.

Для организации эффективной работы дисковой подсистемы сервера в состав сетевых ОС семейства Windows входят следующие служебные программы: «Архивация данных», «Дефрагментация диска» и «Очистка диска». Администратор может настраивать систему на следующие виды архивирования информации:

- обычная архивация, когда после завершения операции архивирования система присваивает файлу метку, согласно которой он добавляется в архив и у него снимается атрибут «Архивный»;

- копирующая архивация, когда у добавляемых в архив файлов атрибут «Архивный» не снимается;
- ежедневная архивация, когда все файлы, которые изменялись в течение дня до выполнения ежедневной архивации, добавляются в архив, при этом атрибут «Архивный» не снимается;
- добавочная архивация, при которой в архив добавляются только те файлы, которые были созданы или изменены со времени последнего обычного или добавочного архивирования; атрибут «Архивный» снимается;
- разностная архивация, при которой в архив добавлены все файлы, созданные или измененные после обычной или добавочной архивации. Атрибут «Архивный» не снимается.

Сетевые ОС семейства Windows имеют группу программ (утилит), которые запускаются из командной строки и используются для решения задач, связанных с оценкой качества работы компьютера в сети. Рассмотрим наиболее важные из этих утилит.

- Утилита ping предназначена для проверки работоспособности участка сети, связывающего исходный компьютер с удаленным компьютером. Если абонент, указанный в запросе утилиты, отвечает на запрос, то участок сети работоспособен, а если сообщение не поступает, то после некоторого таймаута утилита выдает сообщение о том, что связь с абонентом отсутствует. Стандартное значение тайм-аута равно 20 с, но может быть изменено в случае необходимости. Утилита имеет набор опций, управляющих сеансом связи с удаленным абонентом.
- Утилита ipconfig предназначена для отображения на экране монитора основных параметров IP-протокола, используемого в ОС семейства Windows.
- Утилита tracert используется для отображения на экране монитора пути прохождения сигнала от источника до выбранного адресата. Довольно часто это позволяет выяснить причины низкой производительности канала связи.

Промежуточные точки, расположенные в канале связи, после прохождения которых время отклика резко увеличивается, свидетельствуют о наличии в них узких мест, которые не справляются с поступающей нагрузкой.

2.2 Реестр сетевых ОС семейства Windows

При настройке рабочих параметров сетевых ОС семейства Windows для обеспечения эффективного функционирования АСОИиУ администратор часто использует системный реестр.

Системный реестр — это база данных для установки рабочих параметров системы, хранения сведений о конфигурации компьютера и настроек его ОС. Системный реестр не имеет ограничений по объему. Любая ОС семейства Windows во время ее загрузки и работы постоянно обращается к системному реестру, который содержит следующие данные:

- профили всех пользователей, т. е. настройки режима их работы;
- конфигурацию оборудования, установленного на компьютере;
- данные об установленных программах;
- свойства папок;
- данные об используемых портах.

Для работы с системным реестром в ОС существует встроенная утилита, которая называется Registry Editor (редактор реестра) и находится в файле regedit.exe. Утилита имеет небольшой размер (135 Кбайт). Для запуска редактора реестра необходимо выбрать команды «Пуск» и «Выполнить», а затем в появившемся на экране монитора новом окне в поле «Открыть» следует ввести команду regedit.exe. Появится окно редактора реестра, которое состоит из четырех основных областей: строка меню, строка состояния, левая панель и правая панель.

Строка меню содержит пункты меню: File (файл), Edit (редактирование), View (просмотр), Favorites (настройка) и Help (помощь).

В левой панели отображается иерархия реестра, которая организована в виде ключей (разделов) и вложенных ключей (подразделов).

В правой панели показаны текущие значения параметров выбранного раздела или подраздела реестра. Каждый параметр реестра характеризуется именем, отображаемым в столбце Name, типом данных, отображаемым в столбце Type, и значением, отображаемым в столбце Data.

В строке состояния, расположенной внизу окна, указывается полный путь к разделу реестра, в составе которого содержится выделенный параметр.

Команды меню редактора реестра позволяют администратору выполнять определенные действия, например:

- команда Modify (изменить) — изменить данные, содержащиеся в составе параметров реестра;
- команда New (создать) — добавить в реестр новые разделы и параметры строковых типов, двоичные параметры и параметры типа REG_DWORD;
- команда Rename (переименовать) — переименовать значимый элемент реестра;
- команда Delete (удалить) — удалить соответствующий элемент реестра.

Поскольку удаление параметров, разделов и подразделов реестра — это необратимая операция, при удалении следует действовать аккуратно.
Администратор может назначать и изменять следующие права доступа пользователей к разделам реестра: No Access (нет доступа), Full Control (полный доступ), Read (только чтение), Special Permissions (специальный доступ). Полный доступ к разделам реестра обязательно должны иметь члены группы «Администратор» и сама операционная система. Такая установка прав доступа позволяет гарантировать возможность полного восстановления разделов реестра администратором при запуске системы.

Выполнить все основные действия в реестре может только администратор системы или пользователь, имеющий права администратора. Чтобы назначить пользователю определенные права доступа к разделам реестра, администратор должен:

- выполнить резервное копирование тех разделов реестра, на которые следует установить права доступа;
- выделить конкретный раздел реестра, для которого следует установить права доступа;
- в меню редактирования выбрать команду Permissions, а затем в открывшемся диалоговом окне выбрать имя нужного пользователя или группы и установить для них требуемые права. Права, которые может установить администратор для пользователей и их описание приведены в табл. 2.4.

Таблица 2.4

Типы прав доступа к реестру, устанавливаемые администратором для пользователей сетевых ОС Windows

Право доступа	Описание
Read	Позволяет просматривать содержимое соответствующего раздела реестра, не давая сохранять изменения
Full Control	Разрешает получать доступ к соответствующему разделу, редактировать его содержимое и изменять права доступа к нему
Special Permissions	Позволяет индивидуально назначать разные комбинации прав доступа и редактирования к соответствующему разделу

Чтобы дать пользователю права (или комбинацию прав) для специального доступа, администратору следует использовать кнопку Advanced (дополнительно). После этого раскроется диалоговое окно для предоставления соответствующих прав, табл. 2.5.

Таблица 2.5

Типы прав специального доступа к реестру, устанавливаемые администратором для пользователей сетевых ОС Windows

Право доступа	Описание
Query Value	Дает право чтения значений параметров разделов реестра
Set Value	Позволяет устанавливать значения параметров разделов реестра
Create Subkey	Разрешает создавать подразделы в выбранном разделе реестра
Enumerate Subkey	Дает право идентифицировать подразделы выбранного раздела реестра
Notify	Позволяет назначать установки аудита на разделы реестра
Create Link	Дает право создавать символические ссылки в конкретном подразделе
Delete	Разрешает удалять выделенный раздел или подраздел
Write DAC	Позволяет получать доступ к разделу, создавать и модифицировать для него список контроля доступа (Access Control List, ACL)
Write Owner	Дает право присвоения права владельца данного раздела
Read Control	Разрешает просматривать параметры безопасности, установленные для данного раздела или подраздела

Администратор и пользователь с правами администратора могут присвоить себе права владельца на любой раздел или подраздел реестра.

Системный реестр содержит пять основных разделов, приведенных в табл. 2.6.

Таблица 2.6

Разделы системного реестра сетевых ОС Windows и их описание

Раздел системного реестра	Описание
HKEY_CURRENT_USER	В разделе хранятся настройки пользователя, вошедшего в систему, т. е. папки пользователя и настройки панели управления. Эти данные называются профилем пользователя
HKEY_USERS	Содержит все профили пользователей компьютера
HKEY_LOCAL_MACHINE	Включает все настройки, относящиеся к локальному компьютеру (для всех пользователей)
HKEY_CLASSES_ROOT	Является подразделом HKEY_LOCAL_MACHINE\Software. Хранящиеся в разделе сведения обеспечивают открытие необходимой программы при открытии файла с помощью проводника
HKEY_CURRENT_CONFIG	Включает сведения о профиле оборудования, используемом локальным компьютером при запуске системы

Название любого раздела или подраздела реестра начинается со слова HKEY. Основные типы данных системного реестра приведены в табл. 2.7

Таблица 2.7

Типы данных системного реестра сетевых ОС Windows и их описание

Тип данных	Описание
REG_BINARY	Включает в себя двоичные данные; информация хранится в двоичном виде и отображается в шестнадцатеричном формате
REG_DWORD	Представляет собой целые числа размером 4 байт и отображается в двоичном, шестнадцатеричном или десятичном форматах
REG_EXPAND_SZ	Представляет собой строку данных переменной длины
REG_MULTI_SZ	Содержит многострочный текст, удобный для чтения
REG_FULL_ RESOURCE_ DESCRIPTOR	Представляет собой последовательность вложенных массивов, с помощью которой хранятся списки ресурсов оборудования или драйверов

Для управления записями системного реестра нужно открыть соответствующую ветвь реестра и щелчком правой кнопки мыши вызвать контекстное меню, в котором выбрать один из пунктов (переименовать, изменить, изменить двоичные данные, удалить и т. д.). Для каждого параметра и ветви системного реестра можно задавать разрешения на чтение или запись пользователю или группе пользователей. Для этого следует выбрать конкретную ветвь и пункт меню «Правка» — «Разрешения».

Для настройки с помощью реестра рабочих параметров сетевой ОС на оптимальный режим работы администратор должен выполнить следующие действия:

- выбрать соответствующий раздел, а в нем требуемый подраздел реестра;
- выбрать соответствующий параметр в этом подразделе реестра;
- установить для выбранного параметра необходимое значение.

Некоторые параметры системного реестра и их типовые значения, важные для сетевой безопасности системы, приведены в табл.2.8

Таблица 2.8

Параметры системного реестра, важные для обеспечения сетевой безопасности системы

Параметр системного реестра	Описание
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\ \CurrentVersion\Policies\Network] AlphanumPwds=1	Позволяет требовать вводить пароли только из букв и цифр. Может обязать пользователя всегда комбинировать в паролях буквы и цифры
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ \CurrentVersion\Policies\Network] MinPwdLen=hex:6	Обеспечивает установку минимального числа символов в паролях
[HKEY_CURRENT_USER\Software\Microsoft\Windows\ \CurrentVersion\Internet Settings] DisablePasswordCaching=1	Запрещает кэширование паролей
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\ \CurrentVersion\Policies\Network] HideSharePwds=1	Не показывает пароли при вводе. Позволяет заменять символы пароля звездочками
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ \Services\LanmanServer\Parameters] Hidden=1	Позволяет включить режим, при котором в режиме обзора сети другие пользователи не будут видеть ваш компьютер
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ \CurrentVersion\Internet Settings\Cache] Persistent=0	Автоматически удаляет временные файлы после работы в сети Интернет. При значении, равном нулю, обеспечивает удаление всех временных файлов, оставшихся после работы в сети Интернет, а при значении, равном единице, позволит оставить эти файлы на диске
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\ \CurrentVersion\Policies\Explorer] NoInstrumentation=1	Запрещает фиксировать, с какими приложениями недавно работал пользователь и к каким документам получал доступ

Все параметры реестра, касающиеся настройки коммуникационного протокола TCP/IP, находятся в подразделе реестра

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\
\Tcpip\Parameters].

Краткое описание основных параметров и рекомендуемые для них значения приведены ниже:

- EnableDeadcwDetect. Значение этого параметра рекомендуется установить равным нулю, что позволяет протоколу TCP/IP переключаться на дополнительный шлюз в том случае, когда на большое число соединений начинают влиять атаки типа «отказ в обслуживании»;
- EnablePMTUDiscovery. По значению этого параметра протокол TCP/IP определяет максимальный размер передаваемого пакета (Maximum Transfer Unit, MTU). При нулевом значении параметра размер пакета всегда будет равен 576 байт;
- TCPWindowsSize. Задает размер скользящего окна, т. е. число байтов, которое может быть передано узлом источника за один раз без получения подтверждения со стороны узла адресата. Этот размер задается в интервале от MSS до 2^{30} байт, где MSS (Maximum Segment Size) — максимальный размер сегмента, который определяется из выражения MSS = MTU – 40, при этом размер MTU не должен превышать максимальный размер пакета, который, например, для сети Ethernet равен 1500 байт;
- TCP1323Opts. Этот параметр следует установить равным единице в тех случаях, когда размер скользящего окна для TCP-пакетов должен иметь размер более 64 Кбайт;
- Enable PMTUDiscovery. Этот параметр следует установить равным единице, если система сама должна автоматически определять оптимальный размер пакета (MTU), передаваемого по сети, с учетом качества среды передачи данных. Если значение параметра установить равным нулю, то оптимальный размер пакета, передаваемого по сети, должен определять пользователь сети;
- DefaultTTL»=dword:00000080. Это время существования пакета. Если оно будет слишком маленьким, пакет просто не успеет дойти до места назначения, а если слишком большим, то «заблудившиеся» пакеты будут тормозить соединение. В принципе для системы среднего качества связи стандартное значение равно 128. Оптимальное значение определяют экспериментально;

- KeepAlive. Этот параметр указывает, насколько часто система будет осуществлять проверку и верификацию активности открытых соединений. Для него рекомендуется установить значение 300 000.

2.3 Администрирование сетевой ОС Unix

Одной из важных задач администратора сетевой ОС Unix является назначение пользователям прав доступа к каталогам и файлам, которые часто называют объектами. Краткую информацию о каталоге или файле можно получить с помощью команды ls без опций, а полную информацию — команды ls с опцией –l. Полная информация о каталоге или файле выводится на экран монитора и включает слева направо следующие поля данных, которые разделяются пробелами:

- полный набор прав доступа к каталогу или файлу;
- число, которое указывает, сколько раз встречаются в системе ссылки на этот каталог или файл;
- имя владельца данного каталога или файла;
- имена пользователей или группы пользователей каталога или файла;
- размер каталога или файла в байтах;
- дату создания или последней модификации данного каталога или файла, которая включает месяц, число и время (часы и минуты);
- название каталога или файла.

Краткая информация включает только имя каталога или файла.

Например, полная информация о файле lab.cmd может иметь вид:

-rwxr-x--- 1 user1 group1 3500 Avg 22 18:35 lab.cmd.

Администратор может давать пользователям следующие права на доступ к каталогам и файлам:

- право на чтение (read), сокращенно обозначается символом r;
- право на запись (write), сокращенное обознается символом w;
- право на выполнение (execution), сокращенно обозначается символом x.

Комбинацию прав доступа к каталогам или файлам следует указывать в последовательности rwx. Если хотя бы одно из прав у пользователя отсутствует, то на месте этого символа следует ставить прочерк. Например, запись rw означает отсутствие права на выполнение.

Всех пользователей системы по уровню доступа к каталогам и файлам подразделяют на три категории:

- владельцы каталога или файла;
- пользователи, входящие в группу, которой разрешен доступ к этому каталогу или файлу;
- другие пользователи, которые не имеют непосредственного отношения к этому каталогу или файлу.

Полный набор прав доступа представляет собой последовательную комбинацию прав доступа пользователей всех трех указанных категорий. Каждая категория должна быть представлена набором из трех прав доступа на каталог или файл, соответственно чтение

(r) , запись (w) и выполнение (x). Наличие прочерка перед полным набором прав говорит о том, что этот набор прав относится к файлу.

В состав полного набора прав доступа к файлу входят 10 символов:

-	r	w	x	r	w	x	r	w	x
Файл	Права владельца			Права группы			Права других пользователей		

Администратор системы может дать одному и тому же пользователю для разных каталогов и файлов разные категории доступа и разные права. Если пользователь сам создал каталог или файл, то он является его владельцем. При создании пользователем каталога или файла ему по умолчанию система назначает следующие права:

для каталога rwxrwxr-x

для файла - rw-rw-r--

По умолчанию пользователь, создавший файл, может его читать, редактировать, а также сделать его исполняемым. При этом разрешить пользоваться созданным каталогом или файлом группе пользователей может как владелец этого каталога или файла, так и администратор системы.

Возможности, которые дают пользователю комбинации прав доступа к каталогам и файлам, приведены в табл. 2.9.

Таблица 2.9

Возможные права доступа пользователей к ресурсам ОС Unix

Восьмеричный вид	Двоичный вид	Символьный вид	Права доступа
0	000	---	Нет никаких прав
1	001	--x	Только выполнение
2	010	-w-	Только запись
3	011	-wx	Только запись и выполнение
4	100	r--	Только чтение
5	101	r=x	Только чтение и выполнение
6	110	rw	Только чтение и запись
7	111	rwx	Полные права

Администратор может и должен индивидуально устанавливать каждому пользователю права на доступ к каждому каталогу и файлу.

Устанавливать и изменять права доступа пользователей к каталогам и файлам администратор может с помощью команды chmod. При этом он может использовать как восьмеричный, так и символьный виды задания прав доступа пользователей к каталогам и файлам. Опции, которые следует указывать после команды chmod для выполнения соответствующих действий, приведены в
табл. 2.10

Таблица 2.10

Установка администратором прав доступа пользователей
к каталогам и файлам ОС Unix с помощью команды chmod

Опция команды chmod	Назначение команды chmod с данной опцией
+	Устанавливает право доступа
-	Отменяет право доступа
=	Присваивает весь набор прав доступа
U	Устанавливает права доступа к каталогу или файлу для пользователя, который создал его и владеет им
G	Устанавливает права доступа к каталогу или файлу для группы
O	Устанавливает права доступа к каталогу или файлу для других пользователей системы
A	Устанавливает права доступа к каталогу или файлу для владельца, группы и прочих пользователей

Для первоначальной установки права доступа к каталогу или файлу можно использовать команду chmod с опциями восьмеричного вида, приведенными в табл 2.9.

С помощью команды chmod 750 lab.cmd администратор системы устанавливает для файла с именем lab.cmd права доступа -rwxr-x--- согласно которым владелец файла имеет полные права доступа к этому файлу, пользователи группы могут только читать и выполнять этот файл, а другие пользователи не имеют никаких прав доступа.

Для изменения уже имеющиеся права доступа к каталогу или файлу также следует использовать команду chmod, но только с опциями символьного вида. Например, если администратору системы необходимо дать всем другим пользователям системы право на чтение файла lab,cmd, согласно табл 2.9 и 2.10, следует выполнить команду chmod o+r lab.cmd. В этом случае после выполнения команды ls -l lab.cmd полная информации о файле lab.cmd будет иметь вид —rwxr-xr-- 1 user1 group1 3500 Avg 22 18:55 lab.cmd.

Ясно, что администратор изменил права на доступ к файлу lab,cmd

с прав -rwxr-x--- на права -rwxr-xr--.

Следует иметь в виду, что только администратор системы может выполнить следующие действия:

- изменить владельца каталога или файла с помощью команды rool;
- изменить группу пользователей для каталога или файла с помощью команды chgrp. Чтобы для файла lab.cmd заменить текущую группу пользователей с именем group1 на группу пользователей с именем group2, нужно выполнить команду chgrp group2 lab.cmd.

Поскольку довольно часто узким местом АСОИиУ является дисковая подсистема сервера, одной из задач администратора является оценка качества ее функционирования. Для этой цели следует использовать команду instat с ключом -x для вывода расширенной статистики. Команда имеет вид % instat -x. По этой команде на экран монитора выводятся параметры оценки работы дисковой подсистемы сервера, табл. 2.11.

Таблица 2.11

Параметры оценки работы дисковой подсистемы сервера

Параметр	Описание
r/s	Количество операций чтения в секунду
kr/s	Количество прочитанных килобайт в секунду
w/s	Количество операций записи в секунду
Kw/s	Количество записанных килобайт в секунду
Wait	Среднее количество транзакций, ожидающих обслуживания
Actv	Количество запросов, обслуживаемых в настоящее время
Wsvs_t	Среднее время нахождения запроса в очереди (мс)
%w	Процент времени нахождения транзакций в очереди
%b	Процент времени активного обслуживания транзакций

Если производительность дисковой подсистемы сервера мала, то следует увеличить размер буферного кэша. Исходный размер буферного кэша можно определить с помощью следующей команды
/usr/sbin/sysdef I grep bufhwm.

По умолчанию значение параметра bufhwm составляет 2 % размера ОП. Этот параметр определяет максимальный объем ОП, который может использовать буферный кэш. Рекомендуется устанавливать размер буферного кэша не более 20 % размеров ОП.

Сетевая ОС Unix имеет в своем составе группу программ, т. е. утилит, которые запускаются из командной строки и позволяют администратору эффективно решать задачи, связанные с работой компьютера (или сервера) в сети. С помощью этих утилит администратор сети осуществляет диагностику

работы протокола TCP/IP, который используется для организации передачи данных между любыми двумя узлами сети. Наиболее важные утилиты и их описание представлены в табл. 2.12.

Таблица 2.12

Утилиты для диагностики работы оборудования в сети по протоколу TCP/IP

Наименование утилиты	Описание
ping	Предназначена для проверки работоспособности сети и выдачи ответа со стороны того абонента, который указан в ней. Утилита имеет набор опций. Запросы посылаются заданное в утилите число раз либо по умолчанию до тех пор, пока пользователь не введет команду управления «DEL». После этого на экран монитора выводятся статистические данные о работе канала связи. Если абонент отвечает, то сеть работоспособна, а если не отвечает, то связь с абонентом отсутствует
ifconfig	Предназначена для просмотра и управления параметрами сетевых интерфейсов в ОС Unix
traceroute	Позволяет выявить последовательность узлов, состоящих из маршрутизаторов, через которые проходит IP-пакет на пути следования от узла источника к узлу назначения
route	Позволяет выполнять процесс конфигурирования сетевых маршрутных таблиц
netstat	Позволяет отобразить на экране монитора компьютера всю статистическую информацию по текущим соединениям по протоколу TCP/IP
TCPdump	Предназначена для перехвата сетевого трафика. Вклю-чает большой набор опций, позволяющих выбрать как объект перехвата, так и условия перехвата, например: какие пакеты перехватывать
ftp	Протокол передачи файлов осуществляет передачу файлов, а также управляет каталогами на удаленном компьютере

Контрольные вопросы и задания к главе 2

1. Какие утилиты сетевой ОС Netware администратор системы использует в своей работе и с какой целью?
2. Какие команды консоли сервера сетевой ОС Netware администратор системы использует в своей работе и с какой целью?
3. Перечислите права, которые администратор сетевой ОС Netware может дать пользователям для работы с объектами и их свойствами, а также с каталогами и файлами.
4. Перечислите основные типы разрешений ОС семейства Windows.
5. Дайте рекомендации по установке разрешений ОС семейства Windows
6. Перечислите для ОС Windows 8 основные разрешения и составляющие их специальные разрешения.
7. Перечислите функции специальных разрешений Windows 8.
8. Поясните назначение объектов и счетчиков системного монитора в сетевых ОС семейства Windows.
9. Дайте рекомендации по устранению узких мест системы, построенной на основе ОС семейства Windows.
10. Поясните состав и структуру системного реестра ОС семейства Windows.
11. Перечислите права доступа, которые администратор может дать пользователям для работы с системным реестром ОС Windows.
12. Перечислите основные параметры протокола TCP/IP, которые администратор может устанавливать с помощью системного реестра ОС Windows.
13. Перечислите для ОС Unix права доступа к каталогам и файлам, а также категории пользователей, которым эти права могут быть предоставлены.
14. Как можно задать и изменить права доступа пользователя к каталогам и файлам в ОС Unix?
15. Перечислите утилиты, которые может использовать администратор ОС Unix для оценки работы компьютера в сети, и поясните их назначение.

Литература к главе 2

Основная

Щетка П. Microsoft Windows Server 2003. Практическое руководство по настройке сети: пер. с англ. / П. Щепка. СПб.: НИТ, 2006. 608 с.

Дополнительная

Вишневский А. Windows Server 2003 для профессионалов / А. Вишневский. СПб.: Питер, 2004. 767 с.

Джан-Пауло. Настройка производительности UNIX систем: пер. с англ. / Джан-Пауло, Д. Мусумеси, Майк Лукидес. СПб.: Символ Плюс, 2003. 408 с.

Чекмарев А. Windows 7. Руководство администратора / А. Чекмарев. СПб.: БХВ Петербург, 2010. 896 с.

Глава 3. Администрирование систем управления базами данных

3.1 Основы администрирования систем управления базами данных

Администрирование систем управления базами данных (СУБД) предполагает наличие:

- пользователей, работающих с базами данных;
- баз данных, с которыми работают пользователи;
- системы управления базами данных;
- сети, включающей аппаратно-программные средства, обеспечивающие взаимодействие пользователей с базами данных;
- обслуживающего персонала, осуществляющего эксплуатацию системы.

Работать с базами данных может только зарегистрированный пользователь, который обладает соответствующими правами. Система безопасности СУБД имеет встроенную систему защиты, включающую несколько вложенных уровней: СУБД, база данных, объект базы данных.

Администрирование СУБД, как правило, осуществляют следующие специалисты: системный администратор (System Administrator–SA), администратор баз данных (Data Base Administrator- DBA), администратор сети (Network Administrator- NA), разработчик приложений баз данных (Developer Data Base Application-DDBA)

Кроме этого следует отметить следующие категории пользователей баз данных: владелец базы данных, владелец объектов базы данных и пользователь, работающий с объектами базы данных.

Системный администратор – это специалист, в обязанности которого входит обеспечение производительной и отказоустойчивой работы аппаратно-программных компонент, входящих в состав системы, и который решает следующие задачи:

- установка и конфигурирование ОС и необходимых обновлений для ОС и используемых программ;
- установка и конфигурирование нового аппаратного и программного обеспечения;

- установка и настройка аппаратных и программных средств системы для обеспечения эффективности их функционирования;
- установка и настройка рабочих параметров СУБД с целью снижения конкуренции запросов пользователей за используемые ресурсы;
- создание пользователей, работающих в системе;
- обеспечение требуемого режима работы пользователей с базами данных;
- предоставление пользователям адекватных прав доступа (разрешений) , которые обеспечивают им требуемый уровень доступа к папкам, файлам и программам для выполнения порученной работы с базой данных согласно штатному расписанию;
- проведение резервного копирования данных;
- обеспечение конфиденциальности и безопасности данных, находящихся в системе;
- .проведение мониторинга работы аппаратно-программных средств системы.

Администратор баз данных – это специалист, который осуществляет выработку требований к базе данных, её логическое проектирование, физическую реализацию, эффективное использование и сопровождение, включая управление учётными записями пользователей базы данных и ее защиту от несанкционированного доступа.

Администратор баз данных решает следующие задачи:
- установка, обновление, сопровождение и эксплуатация баз данных;
- настройка рабочих параметров баз данных;
- резервное копирование и восстановление баз данных;
- оптимизация производительности баз данных за счет распределения баз данных по дискам с целью предотвращения конкуренции между запросами к дисковой памяти и уменьшения времени доступа к дисковой памяти;
- обеспечение целостности баз данных;

- обеспечение требуемого времени выполнения запросов пользователей к базе данных за счет своевременного выполнения транзакций.

Транзакция – это логический модуль, который состоит из набора изменений (вставок, обновлений, удалений) базы данных, при этом в базе данных фиксируются либо все изменения, задаваемые в транзакции, либо ни одно из них. Распределенная транзакция – это транзакция, которая предусматривает внесение изменений в несколько баз данных.
Следует отметить следующие четыре важных свойства транзакции, которые объединены в аббревиатуру ACID (или АСИД):

1. Atomicity (Атомарность или неделимость). Транзакция выполняется как атомарная операция: либо выполняется вся транзакция целиком, либо она целиком не выполняется.

2. Consistency (Согласованность). Транзакция переводит базу данных из одного согласованного (целостного) состояния в другое согласованное (целостное) состояние.

3. Isolation (Изоляция). Транзакции разных пользователей не должны мешать друг другу.

4. Durability (Долговечность или устойчивость) Если транзакция выполнена, то происходит фиксация транзакции, означающая, что результаты ее работы должны сохраниться в базе данных, даже в случае возможного последующего сбоя в работе системы.

Одной из базовых задач администратора баз данных является резервное копирование данных, обеспечивающее надежное функционирование баз данных. Обычно администраторы баз данных используют следующие виды резервного копирования:

- полное резервное копирование, которое подразумевает копирование всей базы данных, производится обычно один раз в неделю;

- дифференцированное резервное копирование, которое предназначено для записи всех изменений, произошедших в базе данных после выполнения

последнего полного резервного копирования, производится обычно один или два раза в день.

Администратор вычислительной сети – это специалист, отвечающий за работу сети, объединяющей компоненты АСОИиУ в единую систему.

Администратор вычислительной сети решает следующие задачи:

- установка, конфигурирование и поддержка в рабочем состоянии сетевого оборудования;
- назначение сетевых адресов устройствам сети;
- разбиение сети на отдельные подсети с целью увеличения общей производительности работы системы;
- контроль сетевого трафика между узами сети с целью выявления узких мест сети и их последующего устранения;
- настройка рабочих параметров сетевого оборудования (коммутаторов, маршрутизаторов), выбор и настройка рабочих параметров протоколов передачи данных с целью увеличения производительности, надежности и безопасности передачи информации по сети.

Разработчик приложений баз данных – это специалист, который создает программные продукты для использования их с целью обеспечения эффективной работы пользователей с базами данных, Он осуществляет

- сопровождение приложений баз данных;
- выявление и корректное исправление ошибок, обнаруженных в процессе работы приложений;
- настройку приложений на эффективный режим работы с базами данных.

Обычно в процессе эксплуатации АСОИиУ, администратор системы должен взаимодействовать с администратором баз данных при определении необходимых системных ресурсов и их количественного состава, а администратор баз данных взаимодействовать с администратором сети для обеспечения эффективного режима функционирования баз данных в сети и надежного обмена информацией между базами данных и пользователями сети. В то же время разработчик приложений должен взаимодействовать с

администратором баз данных с целью настройки приложений на более эффективный режим работы с базами данных.

Кроме этого, все эти специалисты должны взаимодействовать с администратором сети, чтобы совместно находить варианты минимизации временных задержек при передаче данных по сети, а также способы устранения узких мест сети.

Например, если СУБД будет очень интенсивно использовать оперативную память и администратор базы данных установит слишком большой размер системной глобальной области (System Global Area-SGA) для СУБД, то производительность базы данных увеличится, а производительность системы может снизиться. С другой стороны, если администратор системы установит область SGA слишком малой, система будет работать хорошо, но уменьшится производительность базы данных.

Поэтому для оптимального функционирования компонентов и ресурсов системы, администраторы отдельных направлений должны постоянно и тесно взаимодействовать между собой. Особенно это касается администратора системы и администратора баз данных, которые, как правило, должны совместно решать широкий комплекс вопросов

- выбор СУБД с учетом требований пользователей и возможностей сетевой ОС;
- концептуальное, логическое и физическое проектирование базы данных;
- приемку базы данных в опытную и промышленную эксплуатацию;
- обеспечение физической и логической целостности базы данных;
- тестирование и мониторинг базы данных;
- настройку рабочих параметров СУБД и базы данных при установке и в процессе эксплуатации;
- сбор статистических данных о работе базы данных и оценку характеристик ее производительности;
- восстановление базы данных в случае отказов и сбоев;
- диагностику и устранение ошибок в работе СУБД и базы данных;

- копирование и архивирование базы данных;
- выбор стратегии реорганизации и развития базы данных.

Следует иметь в виду, что в АСОИиУ, при числе пользователей не более 25 человек, как правило, все функции администрирования выполняет один специалист.

Для организации эффективной, производительной и надежной работы системы рекомендуется размещать ее основные программные компоненты: ядро системы, файлы баз данных, файлы журнала транзакций на отказоустойчивых дисковых массивах, учитывая следующие рекомендации:

- файлы сетевой ОС и ядро СУБД следует размещать только на массивах уровня RAID-1, чтобы защитить системные данные;
- файлы базы данных и индексные таблицы - на массивах уровня RAID-5, чтобы обеспечить отличную скорость чтения данных и хорошую отказоустойчивость;
- временные файлы – на массивах уровня RAID-0, чтобы обеспечить отличную скорость чтения и записи данных;
- файлы журнала транзакций – на массивах уровня RAID-1, чтобы обеспечить отличную отказоустойчивость и хорошую скорость чтения и записи данных.

Для проведения сравнительной оценки выбора СУБД при создании АСОИиУ следует учитывать следующие группы критериев:

- функциональные возможности СУБД:

– независимость от аппаратуры и ПО, с которым работает СУБД;

– масштабируемость, т. е. возможность увеличения числа пользователей и объема хранимых данных;

– набор средств, используемых при администрировании;

- контроль работы системы:

– контроль и управление использованием оперативной и дисковой памятью сервера при работе с базой данных;

– возможность автоматической настройки системы на максимальную производительность;

– наличие средств выявления узких мест функционирования системы;

- производительность СУБД:

– рейтинг производительности СУБД с учетом аппаратных средств;

– возможность оптимизации выполнения запросов;

– возможность использования параллельной архитектуры;

- надежность СУБД:

– восстановление системы после сбоев и отказов;

– резервное копирование данных;

– возможности режима «откат транзакций»;

– многоуровневая система защиты данных;

- требования к рабочей среде СУБД:

– поддерживаемые аппаратные средства и требования к оборудованию;

– типы ОС, под управлением которых способна работать СУБД;

- организационно-экономическая эффективность СУБД:

– качество и полнота документации;

– уровень распространения;

– поддержка производителя СУБД;

– стоимость приобретения СУБД;

– стоимость эксплуатации СУБД.

При выборе СУБД также следует учитывать уровень квалификации пользователей и обслуживающего персонала.

Сравнительный анализ ряда промышленных СУБД, с учетом приведенных критериев, показывает, что наибольшее распространение при создании АСОИиУ получили СУБД SQL Server (SQL Server 2005 , SQL Server 2008) и СУБД Oracle. (Oracle 9 g, Oracle 10 g, Oracle 11g)

3.2 Администрирование СУБД SQL Server

Администрирование СУБД SQL Server включает: установку (инсталляцию) СУБД, создание пользователей и задание режима их работы с базой данных, настройку рабочих параметров СУБД и базы данных для обеспечения эффективного функционирования системы.

Инсталляция СУБД SQL Server предусматривает: установку СУБД, базы данных, клиентской части, а также задание их рабочих параметров, например, максимального числа подключенных пользователей, директории для хранения журналов транзакций и сообщений и т. д..

СУБД SQL Server имеет управляющую консоль (Microsoft Management Console), представляющую собой инструмент для организации эффективной работы администратора системы и администратора баз данных и ориентированный на упрощение процесса администрирования.

СУБД SQL Server имеет набор утилит, позволяющих эффективно выполнять большое число функций администрирования СУБД и базы данных. Приведем краткое описание и назначение этих утилит.

Утилита Enterprise Manager — основной инструмент для проведения администрирования СУБД, позволяет осуществлять управление базой данных, выполнять резервное копирование и восстанавливать базы данных, а также проводить репликацию и поддерживать безопасность базы данных на требуемом уровне. Утилита выполняется на компьютере, где установлена СУБД, но также поддерживает управление с удаленного компьютера пользователя. Эта утилита позволяет просматривать и управлять различными компонентами СУБД, представляя все объекты в виде иерархического дерева. Можно не только просматривать объекты, но и управлять конфигурацией сервера. Любое действие над объектом можно выполнить с помощью контекстного меню.

Утилита Distributed Transaction Coordinator управляет распределенными транзакциями, каждая из которых может обращаться к нескольким базам данных, и обеспечивает их фиксацию и откат.

Утилита Query Analyzer представляет собой анализатор запросов и позволяет выполнять SQL-инструкции в интерактивном режиме, а также анализировать выполнение запросов и просматривать статистику плана выполнения запроса.

Утилита SQL Profiler предназначена для сбора и анализа сведений о выполнении запросов, а также трассировки событий, связанных с функционированием сервера базы данных. Утилита регистрирует ошибки и все основные действия над объектами базы данных.

Утилита SQL Performance Monitor предназначена для фиксации текущего состояния сервера базы данных и содержит следующие параметры его работы за последние три секунды:

- число инструкций, выполненных за каждую секунду;
- число страниц, считанных и записанных за каждую секунду;
- число пользователей, подключенных к серверу.

Утилита Data base Consistency Checker предназначена для периодической проверки логической и физической целостности базы данных.

Утилита Bulk Copy Programm предназначена для импорта и экспорта данных между таблицами SQL Server и текстовыми файлами.

Утилита Makepipe предназначена для диагностики соединения клиентов с сервером.

Для организации экспорта и импорта данных в базу данных в составе СУБД имеется служба Data Transformation Services.

СУБД SQL Server имеет встроенную в систему полную справочную документацию и руководство по администрированию сервера базы данных. СУБД имеет также средство создания ER-диаграмм, которое позволяет просматривать и модифицировать структуру таблиц базы данных и их связи, строить диаграммы сущность — связь, но не предназначена для проектирования баз данных. Средство создания ER-диаграмм вызывается и запускается из утилиты Enterprise Manager.

СУБД SQL Server имеет встроенные средства защиты от несанкционированного доступа к данным, которые противостоят таким опасностям, как похищение и фальсификация данных, утрата целостности данных, потеря доступности к данным, находящимся на сервере, и обеспечивают конфиденциальность данных.

Встроенные в СУБД средства мониторинга позволяют администратору баз данных собирать следующую статистику:

- число операций ввода-вывода в единицу времени;
- число соединений, установленных в течение работы СУБД;
- число транзакций в единицу времени;
- число команд процессора, приходящихся на один запрос;
- число команд ввода-вывода, приходящихся на запрос.

По результатам статистических данных администратор может определять «узкие места» и для их ликвидации изменять рабочие параметры СУБД.

Для оптимизации работы СУБД SQL Server администратор имеет возможность настраивать параметры процессора, оперативной памяти и базы данных сервера, а также параметры базы данных клиента, интерфейса пользователя и ядра SQL-сервера.

Возможны два варианта настройки параметров СУБД SQL Server:

- ручная настройка, которая выполняется с помощью утилиты Enterprise Manager. После ее запуска в появившемся окне следует выбрать вкладку «Свойства», а затем в новом открывшемся окне «Конфигурация» следует выбрать ту вкладку, которая соответствует группе рабочих параметров, подлежащих настройке;
- автоматическая настройка, которая выполняется с помощью системной процедуры, имеющий следующий вид: sp_configure (имя параметра настройки), (значение, присваиваемое этому параметру).

Значения всех параметров настройки СУБД SQL Server находятся в системной таблице sysconfigure.

Для внесения изменений в действие необходимо выполнить команду RECONFIGURE с параметром WITH OVERRIDE, который следует указывать только в том случае, когда системному параметру присваивается значение «единица». Наличие параметра WITH OVERRIDE обеспечивает дополнительный уровень защиты и позволяет убедиться в том, что администратор действительно хочет изменить значение соответствующего системного параметра.

Выделяют следующие параметры настройки СУБД SQL Server.

- параметры настройки процессора сервера:

– приоритет для процессора (priority) при обработке запросов СУБД;

– максимальное число рабочих потоков СУБД (max worker threads);

– пороговое время на выполнение запроса в секундах (cost threshold for parallelism), по истечении которого осуществляется переход к параллельному выполнению запросов;

– число потоков для параллельного выполнения запросов (max degree of parallelism);

– максимальное число потоков (max worker threads);

– число процессоров, параллельно выполняющих план (affinity mask);

- параметры настройки оперативной памяти сервера:

– максимальный объем памяти для SQL-сервера (max server memory);

– минимальный объем памяти для SQL-сервера (min server memory);

– минимальный объем памяти, отводимой на один запрос (min memory per query);

- параметры настройки базы данных сервера:

– время сохранения резервной копии (дни) (media retention);

– момент создания очередной контрольной точки (recovery interval);

– число блокировок, поддерживаемых одновременно (Locks);

- параметры настройки базы данных клиента:

– минимальный объем базы данных клиента в килобайтах (data file grow);

– максимальный прирост базы данных клиента в процентах (data file grow by percent);

– максимальный размер журнала транзакций в килобайтах (log file grow);

– максимальный прирост журнала транзакций в процентах (log file grow by percent);

– запрет на прирост базы данных клиента (unrestricted data file grow);

– запрет на прирост журнала транзакций (unrestricted log file grow);

- параметры настройки интерфейса пользователя:

– максимальное число пользовательских процессов, которые могут одновременно подключаться к серверу (user connections);

– максимальное время выполнения удаленного запроса (remote query timeout);

– время ожидания регистрации на сервере до завершения попытки (remote login timeout);

- параметры настройки ядра SQL-сервера;

– максимальное время выполнения запроса на сервере в секундах (query governor cost limit);

– максимальное число одновременно открытых объектов из баз (open objects);

– размер сетевого пакета в килобайтах (network packet size).

Поясним особенности настройки наиболее важных рабочих параметров СУБД SQL Server и дадим рекомендации по их конфигурированию.

Настройка рабочих параметров СУБД SQL Server осуществляется с помощью следующей процедуры:

sp_configure <параметр настройки> <значение параметра настройки>.

Конфигурирование рабочих параметров процессора СУБД SQL Server

Параметр priority boost – устанавливает приоритет обработки запросов СУБД. Если этому параметру присвоено значение 1, то запросы SQL Server будут выполняться в системе Windows под наивысшим приоритетом. Присвоение ей высшего приоритета может вызвать проблемы при запуске на сервере других приложений Windows. Значение этого параметра рекомендуется устанавливать равным 1 только для серверов, непосредственно выделенных под СУБД SQL Server.

- Минимальное значение: 0.
- Максимальное значение: 1.
- Значение по умолчанию: 0.

Параметр max worker threads – устанавливает максимальное число рабочих потоков вычислений, которые система SQL Server сможет использовать. Если установленное значение параметра превосходит число существующих соединений пользователей, для

каждого соединения организуется собственный поток. В противном случае пользователи применяют общий пул рабочих потоков.

- Минимальное значение: 32.
- Максимальное значение: 32 767.
- Значение по умолчанию: 255.

Конфигурирование рабочих параметров ОЗУ СУБД SQL Server

Параметр max server memory - позволяет запретить использование СУБД SQL Server объема оперативной памяти, превышающей указанное значение. Следует оставить значение параметра заданное по умолчанию, если хотите, чтобы СУБД SQL Server динамически захватывала и освобождала память. Если хотите, чтобы постоянно использовался заданный фиксированный объем памяти, то следует задать одинаковые значения для этого параметра и параметра min server memory.

- Минимальное значение: 0.
- Максимальное значение: 2 147 483 647.
- Значение по умолчанию: 2 147 483 647.

Параметр min server memory - обеспечивает использование системой SQL Server объема оперативной памяти не ниже указанного значения. Для организации работы SQL Server с заданным фиксированным объемом памяти следует присвоить параметрам max server memory и min server memory одинаковые значения.

Установка минимального значения памяти для размещения СУБД позволяет избежать уменьшения производительности сервера при захвате памяти другими приложениями.

- Минимальное значение: 0.
- Максимальное значение: 2 147 483 647.
- Значение по умолчанию: 0.

Параметр min memory per query - позволяет установить минимальный объем памяти, выделяемой для выполнения запроса. Увеличение его значения может существенно повысить скорость обработки запросов, включающих выполнение сортировки или хеширования.

- Минимальное значение: 0.
- Максимальное значение: 2 147 483 647.
- Значение по умолчанию: 1 024.

Конфигурирование рабочих параметров базы данных СУБД SQL Server

Параметр media retention - устанавливает число дней хранения каждой созданной резервной копии системы. По истечении указанного периода данная копия может быть

перезаписана. Если будет сделана попытка перезаписать носитель раньше, то система выведет соответствующее предупреждающее сообщение.

- Минимальное значение: 0.
- Максимальное значение: 365.
- Значение по умолчанию: 0.

Конфигурирование рабочих параметров клиентской базы данных СУБД SQL Server

Параметр Data file grow – устанавливает минимальный размер клиентской базы данных в килобайтах

- Минимальное значение: 0 .
- Максимальное значение: 500
- Значение по умолчанию: 3

Параметр Data file grow by percent – устанавливает максимальный прирост клиентской базы данных в процентах

- Минимальное значение: 1.
- Максимальное значение: 100
- Значение по умолчанию: 10

Параметр Unrestricted data file grow – устанавливает запрет на прирост клиентской базы данных, если параметр равен нулю.

- Минимальное значение: 0.
- Максимальное значение: 1
- Значение по умолчанию: 0

Конфигурирование рабочих параметров пользовательского соединения СУБД SQL Server

Параметр user connections - позволяет установить максимальное количество пользовательских процессов, которые могут одновременно подключиться к серверу. Если значение параметра равно нулю, то ограничений на количество подключений пользователей нет. Если максимальное количество соединений пользователей будет превышено, то система выдаст сообщение об ошибке и новое соединение установить будет невозможно до тех пор, пока не освободится одно из уже существующих.

Не рекомендуется устанавливать значение этого параметра большим, поскольку на каждое соединение пользователя заранее выделяется около 12 Кбайт оперативной памяти независимо от того, установлено оно или нет. Значение параметра следует установить

равным максимальному ожидаемому числу пользователей, чтобы не использовать лишнюю память и не создавать неудобства пользователям.

- Минимальное значение: 0.
- Максимальное значение: 32 767.
- Значение по умолчанию: 0.

Конфигурирование рабочих параметров ядра СУБД SQL Server

Параметр network packet size - позволяет установить размер пакета данных, передаваемых по сети. Производительность сети может быть увеличена за счет увеличения размеров сетевых пакетов, формируемых в системе SQL Server. Значение параметра 4 096 байт, устанавливаемое по умолчанию, вполне приемлемо для большинства приложений. Изменять значение размера пакета следует очень осторожно, при этом каждый раз проверять, действительно ли достигнуто увеличение производительности.

Рекомендуется также устанавливать размер пакета кратным размеру пакета передаваемого в сети, чтобы сократить время на его фрагментацию.

* Минимальное значение: 512.
* Максимальное значение: 65 532.
* Значение по умолчанию: 4 096.

Параметр query governor cost limit - позволяет установить максимальную продолжительность времени выполнения запроса в секундах на сервере. По умолчанию параметру присваивается значение 0, означающее отсутствие ограничений.

- Минимальное значение: 0.
- Максимальное значение: 2 147 483 647.
- Значение по умолчанию: 0.

При изменении параметров настройки СУБД SQL Server нужно соблюдать следующие правила:

- обязательно сохранить прежние значения изменяемых параметров СУБД;
- параметры, подлежащие изменению, следует устанавливать поочередно, желательно по одному, но не более трех одновременно, чтобы определить влияние изменения каждого из параметров на производительность СУБД;
- численные значения параметров, подлежащих изменению, не должны очень резко отличаться от прежних значений, их следует изменять в небольших пределах и за несколько циклов.

3.3 Администрирование СУБД Oracle

Среди основных свойств СУБД Oracle следует отметить следующие:

- надежность;
- возможность разбиения крупных баз данных на разделы, что дает возможность эффективно управлять гигантскими гигабайтными базами;
- наличие универсальных средств защиты информации;
- наличие эффективных методов обработки запросов;
- возможность распараллеливание операций в запросе;
- наличие широкого набора средств администрирования.

Инсталляция СУБД Oracle осуществляется запуском файла INIT.ORA, в котором администратор системы и администратор баз данных должны установить значения целого ряда параметров для настройки СУБД и базы данных на требуемый режим работы. К числу основных параметров настройки следует отнести следующие:

DB_NAME <имя базы данных> - для задания имени базы данных следует использовать символы алфавита, цифры, символы подчеркивания, знак диеза и доллара, применение всех остальных символов недопустимо.

DB_FILES <значение> - задает максимальное число файлов базы данных, которые могут быть открыты во время работы системы, рекомендуется установить значение параметра не менее 100.

DB_BLOCK_BUFFERS <значение> - задает суммарное количество блоков для буферного кэша. Умножив этот параметр на параметр

DB_BLOCK_SIZE, получим размер области буферного кэша в байтах .Эта величина вместе с величинами, указанными в SHARED_POOL_SIZE и LOG_BUFFER не должна превышать 50% ОЗУ сервера

DB_BLOCK_SIZE <значение> - задает размер блока базы данных, который рекомендуется делать кратным размеру блока ОС и установить значение 4096 байт или 8192 Кбайт. Следует помнить, чтобы изменить размер блока базы данных, следует удалить всю существующую базу данных, а затем создать ее заново.

LOG_BUFFERS <значение> - задает размер буферов для журнала восстановления, расположенного в системной глобальной области, рекомендуется установить значение параметра кратным значению параметра DB_BLOCK_SIZE, но не менее 1 Мбайт.

SORT_AREA_SIZE <значение> - задает размер области сортировки (в байтах). Эта область предназначена для выполнения команды create index и выполнения запросов с выражениями order by и group by. По умолчанию устанавливается значение параметра 65535 байт, т. е. 64 Кбайт, которое, как показывает практика, явно недостаточно. Рекомендуется установить значение параметра кратным 64 Кбайт, но в пределах от 131072 байт , т .е. 128 Кбайт до 524288 байт, т. е. 512 Кбайт.

OPEN_CURSORS <значение> - задает максимальное количество курсоров, которые могут быть открыты в одном сеансе связи пользователя с базой данных, по умолчанию значение параметра 50, рекомендуется увеличить значение параметра, но установить значение параметра не более 250.

PROCESSES < значение> - определяет максимальное количество процессов, которое одновременно может подключаться к базе данных, рекомендуется установить значение параметра не менее 200.

SESSIONS <значение> - задает максимальное количество одновременных сеансов работы пользователей с базой данных, рекомендуется оставить значение по умолчанию 115.

TIMED_STATISTICS <значение> - задает режим сбора статистики, рекомендуется установить значение TRUE для сбора статистики при отладке базы данных

JOB_QUEUE_INTERVAL <значение> - задает интервал времени в секундах неудачной попытки репликации базы данных. Чтобы не загружать сервер, рекомендуется установить значение параметра в границах не менее 600 (10 мин) , но не более 3600 (1 час).

DB_FILE_MULTIBLOCK_READ_COUNT <значение> - задает максимальное количество блоков, считываемых в одной операции ввода-

вывода в ходе последовательного чтения данных .Значения параметра не должно превышать значения, установленного в операционной системе, и не должно превышать значения DB_BLOCK_BUFFERS/ 4 , которое установлено ранее.

TRANSACTION_PER_ROLLBACK_SEGMENTS <значение> - задает максимальное количество транзакций, которые могут использовать один сегмент отката одновременно, рекомендуется оставить значение по умолчанию.

LOG_SIMULTANEOUS_COPIES <значение> - задает максимальное количество защелок копирования буферов восстановления, доступных для одновременной записи входов журнала, рекомендуется оставить значение по умолчанию

LOG_CHECKPOINT_TIMEOUT <значение> - задает время между выполнением контрольных точек, рекомендуется оставить значение по умолчанию, равное 0.

OPTIMIZER_MODE <тип оптимизатора запросов>- задает тип оптимизатора выполнения запросов (плана выполнения запросов), который будет использован при работе СУБД.

Рекомендуется использовать тип <CHOSE> - оптимизатор по стоимости, как наиболее приемлемый с экономической точки зрения.

Можно устанавливать и использовать другие оптимизаторы запросов: <ROLE> -продукционный оптимизатор, <FIRST_ROWS> - оптимизатор увеличивающий производительность выполнения запроса, <ALL_ROWS> - оптимизатор сокращающий общее время выполнения запроса.

PRE_PAGE_SGA <значение> - задает режим страничного обмена с системной глобальной областью памяти. Рекомендуется установить значение <Yes> , что заставляет СУБД Oracle переносить все страницы системной глобальной области в память и тем самым увеличивать производительность работы системы.

SHARED_POOL_SIZE <значение> - задает размер области памяти, в которой содержатся совместно используемые курсоры и хранимые процедуры SQL. Для производительной работы системы рекомендуется установить значение параметра не менее 30 Мбайт.
Администратору баз данных Oracle также рекомендуется использовать программу Automatic Shared Memory Management для конфигурации рабочих параметров с целью уменьшения дисковых операций чтений, сортировки и перестроения Особого внимания заслуживает параметр: SGA_MAX_SIZE <значение>, который задает в процентах при установке системы объем оперативной памяти, доступный базе данных, рекомендуется устанавливать значение в пределах 60-80%.

В системе может быть несколько баз данных, но каждая из них должна иметь свое имя.

После установки системы и создания базы данных администратор баз данных создает для каждой базы данных пользователей (учетные записи пользователей), используя команды:

CREATE USER <имя пользователя>
IDENTIFIED by <пароль>

Учетная запись пользователя включает: имя пользователя; пароль доступа к системе; размер табличного пространства, в котором пользователь может создавать объекты базы данных; привилегии и т. д.

Администратор баз данных должен дать каждому пользователю необходимые привилегии системного и объектного уровней, позволяющие пользователю использовать команды СУБД и работать с объектами базы данных, создавать и изменять их.

Привилегии системного уровня, которых более 80, позволяют пользователю в своей работе использовать определенные команды СУБД SQL server, а привилегии объектного уровня позволяют работать с объектами базы данных и выполнять с ними соответствующие действия

Следует иметь в виду, что пока пользователь не получит по меньшей мере одну привилегию системного уровня, он не сможет работать с базой данных. Основная привилегия системного уровня, которую должна иметь учетная запись каждого пользователя, это CREATE SESSION – возможность создания сеанса связи пользователя с базой данных;

Для создания процедур и создания таблиц в составе базы данных, пользователь должен иметь соответственно следующие привилегии системного уровня: CREATE PROCEDURE, CREATE TABLE

Для предоставления пользователю привилегии системного уровня администратор базы данных использует команду GRANT, указывая при этом название привилегии и имя пользователя, которому она предоставляется.

Для предоставления какой-либо привилегии системного уровня всем пользователям базы данных (существующим и создаваемым в будущем), вместо имени конкретного пользователя следует указать слово <PUBLIC> .

К основным привилегиям объектного уровня, которые администратор базы данных может предоставить пользователю, следует отнести следующие:

ALL- предоставление всех привилегий объектного уровня;

ALTER – изменять таблицы;

DELETE – удалять из таблицы строки;

EXECUTE – вызывать процедуры обмена;

INDEX – создавать индексы на таблицах владельца;

INSERT- вставлять строки в таблицу;

SELECT – делать запрос к данным таблицы базы данных;

REFERENCES – обращаться к объектам другого пользователя;

UPDATE – обновлять строки в таблице.

Для предоставления пользователю привилегии объектного уровня администратор базы данных использует команду GRANT, указывая при этом название привилегии объектного уровня и имя пользователя, которому она предоставляется.

Для изъятия у пользователя привилегии системного (или объектного) уровня администратор базы данных использует команду REVOKE, указывая при этом название изымаемой привилегии и имя пользователя, у которого она изымается.

Несколько привилегий одного уровня администратор базы данных может объединить в роли. Роли – это совокупность привилегий системного и объектного уровней, которые были сгруппированы администратором базы данных под одним именем, чтобы существенно упростить процесс предоставления и отмены этих привилегий у пользователей. Для создания роли используется команда: CREATE ROLE <имя роли>, а для удаления роли команда: DROP ROLE <имя роли>. Для предоставления пользователю или сразу нескольким пользователям одинаковых ролей (набора одинаковых привилегий) используется команда GRANT.

Для смены пароля пользователя, размера заданного по умолчанию табличного пространства и квоты памяти, используется следующая команда: ALTER USER <имя пользователя>.

IDENTIFIED by <пароль>

Пример 3.1 Создайте пользователей us1, us2, us3 соответственно с паролями привет1, привет2, привет3 и предоставьте каждому из них по три привилегии системного уровня

Решение.
```
SQL> CREAFE USER us1
        IDENTIFIED by привет1
     CREAFE USER us2
        IDENTIFIED by привет2
     CREAFE USER us3
        IDENTIFIED by привет3
SQL> GRANT CREAFE SESSION,
           CREATE TABLE,
           CREATE PROCEDURE,
           TO us1, us2, us3.
```

Для выявления узких мест системы с целью уменьшения времени реакции системы на запросы пользователей и увеличения производительности работы, администратору систему и администратору баз данных следует использовать программу Oracle Sever Manager, которая входит в состав программного обеспечения СУБД и является ценным инструментальным средством, способствующим поиску узких мест в базе данных. В графическом режиме программа поддерживает мониторы: канала связи; планировщика; ввода-вывода файлов; защелки; кэша библиотеки; блокировки; процесса; очереди; отката; сеанса; совместно используемого сервера; области SQL; системного ввода-вывода; системной статистики; доступа к таблицам; табличного пространства Эти мониторы довольно просты в использовании, а процесс их запуска почти идентичен.

Программа Oracle Sever Manager позволяет получить статистические отчеты об использовании файлов базы данных и оценить следующие параметры:

- уровень конкуренции за использование глобальной системной области памяти;
- среднее время доступа к дискам;
- среднее время работы центрального процессора;
- уровень использования ресурсов базы данных, таблиц, индексов и т. д..

База данных Oracle содержит большой набор динамических таблиц, которые помогают администратору базы данных оценить производительность работы основных компонент системы. Рассмотрим назначение некоторых основных таблиц:

- таблица VSSESS1ON_WAIT содержит информацию, помогающую контролировать настройки базы данных и выявить проблемы с центральным процессором, памятью, дисками, файлами, а также проблемы конкуренции за ресурсы базы данных, оценить задержки к процессору, памяти, дискам;
- таблица VSDATAFILE содержит информацию, помогающую контролировать настройки дискового ввода-вывода базы данных, однако она доступны только пользователю SYS и любому пользователю, которому предоставлена привилегия SELECT ANY TABLE.
- таблица VSWAITSTAT содержит информацию, позволяющую контролировать конкуренцию за сегменты отката. Сегменты отката выполняют важную роль по хранению всей информации, необходимой для отмены транзакции до ввода на диск всех обновлений. Поскольку сегменты отката должны хранить всю эту информацию, они устанавливаются по размеру в соответствии с типичными транзакциями, которые имеют место в базе данных.

В табл. 3.1 приведены значения числа сегментов отката, которые рекомендуется иметь для базы данных Oracle, в зависимости от числа одновременно происходящих транзакций.

Таблица 3.1

Выбор числа сегментов отката для базы данных Oracle

Число одновременно происходящих транзакций	**Рекомендуемое количество сегментов отката**
1-16	**4**
17-32	**8**
33 и более	**12**

Важной частью базы данных, кроме сегментов отката, являются журналы восстановления.. В них фиксируются все изменения данных, которые могут использоваться для восстановления базы данных, если разрушится либо она, либо вся система Конкуренция за журналы

восстановления очень редко приводит к потере производительности, хотя такая возможность существует.

Для того, чтобы процесс мог выполнить запись в буферы журнала восстановления, он должен приобрести *защелку*, которая представляет собой метку-заполнитель в памяти. Как только защелка приобретена, оператор языка SQL, выполняемый процессом, записывается в журнал восстановления, а затем выполняется. Если транзакция завершается успешно, то буфер журнала восстановления записывается на диск. Если процесс не может получить защелку, он должен ожидать небольшое время.

База данных Oracle должна иметь два или более файлов журнала восстановления. По мере заполнения буфера журнала восстановления он выводится в один из файлов журнала восстановления. Как только файл журнала восстановления будет заполнен, буфер журнала начинает записывать в другой файл журнал. Если существуют несколько файлов журнала, то база данных циклически обращается к каждому из них, прежде чем возвратится к первому файлу журнала восстановления.

Рекомендуется использовать такой вариант организации журнала восстановления, при котором имеются два файла журнала восстановления, распределенные по двум отдельных дискам, которые не содержат других файлов базы данных. Записи архивных журналов следует разместить на третьем диске. Важно, чтобы не было конкуренции между запросами к файлам журнала восстановления и файлам базы данных.

Поэтому следует соблюдать следующие два правила для организации работы журнала восстановления:

• не рекомендуется хранить два последовательных файла журнала восстановления на одном и том же диске,

• число файлов журнала восстановления должно быть кратным числу дисков, используемых для их хранения, с целью выравнивания загрузки дисков

Особое внимание следует уделить организации работы системной глобальной области (System Global Area- SGA) памяти СУБД Oracle.

Рекомендуется системную глобальную область памяти СУБД Oracle полностью размещать в оперативной памяти, чтобы обеспечить оптимальную производительность всей системы Если же всю область SGA не удается разместить в оперативной памяти системы и часть SGA будет размещена на диск, то база данных будет работать менее эффективно, чем это возможно. Если установить в файле init.ora параметр PRE_PAGE_SGA = YES, то можно автоматически считывать всю область SGA в оперативную память при запуске базы данных. Уменьшение размера области SGA, как правило, приводит к снижению производительности.

Чтобы знать, сколько оперативной памяти распределено для области SGA, можно воспользоваться следующей командой:

SVRMGR> SHO W SGA

Системная глобальная область памяти состоит из четырех частей: буферный кэш базы данных, буфер журнала восстановления, совместно используемый пул и курсоры.

Буферный кэш базы данных – это область памяти, которая обеспечивает хранение блоков данных, считанных с диска и которые наиболее часто используются. Он также хранит все изменения, которые еще не были записаны на диск.

Параметр DB_BLOCK_SIZE файла INIT.ORA определяет размер буферов баз данных при создании базы данных, а параметр DB_BLOCK_BUFFERS файла INIT.ORA определяет число буферов баз данных. Полученное произведение значений этих параметров представляет собой общий объем памяти, который занимает буферный кэш базы данных.

Буфер журнала восстановления - это область памяти, в которой хранится вся информация восстановления перед ее записью в файлы журнала восстановления. Этим размером управляет значение параметра LOG_BUFFER файла INIT.ORA, который задается в байтах и должен быть кратным параметру DB_BLOCK_SIZE. Таблица SYS.VSSYSSTAT содержит статистические данные о работе буфера журнала восстановления

Для устранения конкуренции за буфер журнала восстановления следует увеличить значение параметра LOG_BUFFER в файле INIT.ORA

Совместно используемый пул - это область памяти в SGA, отведенная для областей SQL, для пакетов и процедур PL/SQL, а также для информации блокировки, словаря данных и кэша библиотеки. Она содержит три области:

- информация кэша библиотеки;
- информация кэша словаря;
- информация сеанса.

Размер совместно используемого пула определяется значением параметра SHARED_POOL_SIZE файла INIT.ORA и измеряется в байтах

Курсоры — это дескрипторы или указатели на область SQL в области SGA. Чем больше курсоров будет открыто для сеанса, тем больше потребуется памяти для этого сеанса, что в свою очередь означает более высокие требования к памяти, предъявляемые приложением. Если открыто слишком много курсоров, то Oracle может начать выгружать информацию из совместно используемого пула, пытаясь отвести больший объем памяти для курсоров.

При задании курсоров следует соблюдать следующие принципы:

• по возможности явно открывайте курсор;

• если нет недостатка в памяти, не закрывайте курсор при условии, что он будет использоваться снова;

• явно закрывайте курсор, полностью закончив с ним работу;

• ограничивайте число одновременно открытых курсоров с целью ограничения требований к памяти.

Следует иметь в виду, что база данных очень интенсивно использует дисковый ввод-вывод, поскольку большинство операций связано с чтением информации с дисков и записью на них для сохранения или выборки данных.

При установке и настройке файлов базы данных, с целью увеличения производительности работы дисковой подсистемы, следует соблюдать следующие правила:

• создавать отдельные табличные пространства для таблиц и индексов;

• размещать табличные пространства таблиц и индексов на разных физических дисках;

• хранить журналы восстановления и сегменты отката на разных дисках;

• помещать выполнимые программы Oracle и файлы данных базы данных на разные диски;

• наиболее загруженные таблицы, индексы и их табличные пространства помещать на отдельные физические диски;

• распределять физические диски между несколькими дисковыми контроллерами для обеспечения наилучшей производительности дискового ввода-вывода;

• не устанавливать пакеты программ других разработчиков на диски с данными Oracle.

Контрольные вопросы и задания к главе 3

1.Перечислите специалистов, которые осуществляют администрирование СУБД, и набор функций, которые должен выполнять каждый из них.
2. Дайте определение транзакции и поясните ее основные свойства.
3. Перечислите виды резервного копирования, которые обычно используют при работе СУБД, а также их достоинства и недостатки.
4. Перечислите основные компоненты дисковой подсистемы, которые следует учитывать при организации эффективной, производительной и надежной работы СУБД.
5. Поясните на примере необходимость взаимодействия администраторов системы, баз данных и сети при администрировании СУБД.
6. Перечислите основные критерии выбора СУБД.
7. Перечислите утилиты, которые должен использовать администратор баз данных при эксплуатации СУБД SQL Server и дайте им краткую характеристику.

8 Поясните, какие статистические данные, необходимые администратору баз данных, позволяют собирать встроенные в СУБД SQL Server средства мониторинга.

9.Перечислите основные параметры настройки СУБД SQL Server на оптимальный режим работы.

10. Перечислите особенности и правила настройки параметров СУБД SQL Server на оптимальный режим ее работы.

11. Перечислите основные параметры настройки СУБД Oracle.

12. Поясните особенности создания учетных записей пользователей в СУБД Oracle.

13. Поясните принципы назначения привилегий и особенности их присвоения пользователям в СУБД Oracle.

14. Поясните различие привилегий системного и объектного уровней в СУБД Oracle.

15. Поясните назначение и особенности использования программы Oracle Server Manager.

16. Поясните назначение динамических таблиц СУБД Oracle и приведите примеры их использования.

17. Поясните назначение и особенности использования журнала восстановления СУБД Oracle.

18. Поясните назначение и особенности использования сегментов отката СУБД Oracle.

19. Приведите состав и дайте рекомендации по организации работы системной глобальной области памяти СУБД Oracle.

20. Перечислите правила, которые следует использовать при установке и настройке файлов базы данных, с целью увеличения производительности работы дисковой подсистемы СУБД Oracle.:

Литература к главе 3

Основная

Беленькая Н.М. Администрирование в информационных системах / Н.М. Беленькая, С.Т. Малиновский, И.В. Яковенко. М.: Горячая линия Телеком, 2011. 400 с.

Дополнительная

Волошина В.Н. Организация баз данных: учеб. пособие. Часть 2./ В.Н. Волошина, С.И. Годеев. Владивосток: Дальневост. Федерал. ун-т., 2011.504 с.

Култыгин О.П. Администрирование баз данных. СУБД SQL Server: учеб. пособие. / О.П. Култыгин. М.: Московская фин. пром. академия, 2012. 230 с.

Глава 4 Организация защиты информации в АСОИиУ

4.1 Правовое обеспечение и стандартизация в сфере защиты информации.

Поскольку сфера информационных технологий постоянно развивается, то также непрерывно совершенствуются и законодательные меры, используемые в этой сфере.

Основополагающими документами по защите информации в Российской Федерации являются:

- Конституция Российской Федерации от 25 декабря 1993 (принята всенародным голосованием 12 декабря 1993 года) с изменениями и поправками от 30 декабря 2008 года.
- Концепция национальной безопасности Российской Федерации, которая утверждена 14 января 2000 года Президентом Российской Федерации. В ней сформулированы важнейшие направления государственной политики РФ в области безопасности.
- Доктрина информационной безопасности Российской Федерации, которая утверждена 9 сентября 2000 года Президентом Российской Федерации

№ Пр-1895. Это совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности в РФ. «Информационная безопасность - это состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства». В содержании Доктрины особо следует обратить внимание на организационно-технические и правовые методы обеспечения информационной безопасности.

Организационно-технические методы обеспечения информационной безопасности включают: создание системы информационной безопасности и ее постоянное совершенствование, предотвращение несанкционированного доступа к обрабатываемой информации, контроль за действиями персонала, имеющего доступ к информации, подготовка кадров в области обеспечения информационной безопасности;

Правовые методы обеспечения информационной безопасности предусматривают разработку правовых актов, регламентирующих отношения в сфере информационных технологий (ИТ) и разработку нормативных методических документов по вопросам информационной безопасности.

Уровни правового обеспечения защиты информации, типовой процесс и основные этапы создания эффективной комплексной системы защиты информации в АСОИиУ приведены в Приложении 1..

Организация защиты информации в АСОИиУ предполагает ее полное соответствие требованиям стандартов компьютерной безопасности.

Один из первых стандартов в сфере защиты компьютерной информации, был разработан Министерством обороны США и Национальным комитетом компьютерной безопасности. Этот документ называется «Критерии оценки доверенных компьютерных систем», который, с учетом цвета обложки, часто называют "Оранжевая книга".

Система безопасности, изложенная в «Оранжевой книге». поддерживает четыре уровня безопасности D (низший уровень), C, B, A (высший уровень) и включает семь классов безопасности D1, C1, C2, B1, B2, B3 , A1, которые соответствуют этим уровням. При этом система безопасности каждого класса должна соответствовать всем требованиям низшего класса и поддерживать все требования своего класса.

Страны Европы (Франция, Германия, Нидерланды и Великобритания) разработали критерии безопасности работы вычислительных систем и назвали их «Критерии оценки безопасности информационных технологий» (Information Technology Security Evaluation Criteria – ITSEC).

Эти критерии известны также и как «Гармонизированные критерии безопасности европейских стран», они содержат семь уровней безопасности от E0 до E6 соответственно в порядке возрастания требований к безопасности и 11 классов безопасности.

В 2000 году был разработан международный стандарт ISO 17799 – «Практические рекомендации по управлению безопасностью информации» («Code of practice for information security management»).

В это же время также был разработан еще один международный стандарт ISO/IEC 15408 – «Общие критерии оценки безопасности информационных технологий» («Common Criterion for Information Technology Security Evaluation»), который обычно называют сокращенно «Общие критерии», получивший достаточно широкое распространение.

Документ «Общие критерии» содержит два основных вида требований безопасности, предъявляемых к информационной системе:

- функциональные требования, которые предъявляются к функциям безопасности системы и реализующим их механизмам;
- требования доверия, которые предъявляются к технологии и процессам разработки и эксплуатации системы.

В отличие от «Оранжевой книги», «Общие критерии» не содержат заранее выделенных классов безопасности. В документе «Общие критерии» угрозы безопасности для информационной системы характеризуются следующими параметрами: источник угрозы, метод воздействия угрозы, уязвимые места системы для угрозы, ресурсы системы, которые подвергаются угрозе.

Гостехкомиссией России также разработан и опубликован ряд руководящих документов, посвященных вопросам защиты информации от несанкционированного доступа. Согласно этих документов, в России предусмотрены три группы и девять классов защищенности автоматизированных информационных систем (АИС) от несанкционированного доступа к информации. При этом каждый класс защищенности АИС характеризуется определенной совокупностью требований к средствам защиты.

В пределах каждой группы соблюдается иерархия классов защищенности АИС. В документах используются следующие обозначения: цифра – номер группы, а буква - номер класса внутри группы. Например: 1А - класс «А» первой группы, 1Б - класс «Б» первой группы и т.д..

Группа «1» имеет высшую степень защищенности среди всех групп. Класс «А» соответствует высшей степени защищенности в группе, а класс «Б» следующий по важности класс защищенности в группе и т. д..

Особенности групп защищенности АИС состоят в следующем:

- первая группа включает многопользовательские АИС, в которых одновременно обрабатывается и хранится информация разных уровней конфиденциальности. Пользователи имеют разные права доступа, а группа содержит пять классов 1А, 1Б, 1В, 1Г, 1Д;
- вторая группа включает многопользовательские АИС, в которых пользователи имеют одинаковые полномочия доступа ко всей информации, обрабатываемой и хранимой в АИС,, на носителях различного уровня конфиденциальности, а группа содержит два класса 2А и 2Б;
- третья группа включает АИС, в которых работает один пользователь, допущенный ко всей информации, размещенной на носителях одного уровня конфиденциальности, группа содержит два класса. 3А и 3Б.

Анализ документов, касающихся вопросов стандартизации защиты компьютерной информации, показывает, что все документы имеют практическую ориентацию и направлены на решение следующих проблем:

- оценка степени угроз информационной безопасности ИС;
- организация информационной безопасности ИС;
- организация многоуровневой защиты информации в ИС.

4.2 Организация информационной безопасности АСОИиУ

Согласно ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения», защита информации представляет собой деятельность по предотвращению утечки защищаемой информации и несанкционированных воздействий на нее. Целью защиты информации является сокращение ущерба для владельцев и пользователей защищаемой информации в результате ее возможной утечки или искажения.

Защита информации — это комплекс технических и организационных мероприятий, направленных на обеспечение информационной безопасности и нейтрализацию угроз информационной безопасности.

ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» (Information technology. Code of practice for information security management) содержит определение информационной безопасности (ИБ). ИБ вычислительных систем — это защищенность данных и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера. Информационная безопасность предусматривает обеспечение конфиденциальности, целостности и доступности информационных ресурсов и поддерживающей их инфраструктуры.

Конфиденциальность информации означает защиту информации от несанкционированного доступа.

Целостность информации означает, что данные, которые находятся на сервере сети, обладают свойствами непротиворечивости, защищенности и актуальности. При этом актуальность подразумевает, что значения данных соответствуют текущему состоянию объекта, который они описывают.

Доступность информации означает, что легальный авторизованный пользователь сети имеет возможность в приемлемое время получить требуемую ему информацию, находящуюся на сервере сети.

Базовая модель, разработанная Р. Клеменсом, и предназначенная для описания набора параметров, которые следует учитывать при организации системы информационной безопасности АСОИиУ, имеет следующий вид:

$$S=(R,Y, Z,V, B) \quad (4.1)$$

где: S- набор параметров информационной безопасности системы;

R - набор защищаемых ресурсов информационной системы;

Y - набор угроз информационной системы;

Z - набор средств защиты для обеспечения информационной безопасности;

V - набор уязвимых мест в составе ресурсов системы, представляющих собой пути для возможного проникновения потенциальных угроз в информационную систему;

B - набор барьеров, представляющих собой места в информационной системе, в которые следует установить средства защиты для обеспечения защиты информации от возможной реализации угроз.

Как правило, в состав защищаемых ресурсов включают все информационные ресурсы, а также системы связи, технические и программные средства обработки информации и помещения, в которых расположены ресурсы системы, подлежащие защите.

Угроза — это потенциальная возможность нарушить информационную безопасность. Попытка реализации угрозы называется атакой, а тот, кто ее предпринимает, является злоумышленником.

Под угрозой информационной безопасности обычно понимают возможность нарушения физической целостности информации или ее логической структуры, а также возможность несанкционированного доступа к информации, ее модификации, удаления и размножения.

Компьютерные угрозы делят на следующие два вида:

- неумышленные угрозы, которые имеют место в следующих случаях:

– ошибочные действия сотрудников при эксплуатации систем вследствие их недостаточной квалификации или безответственности;

– недостаточная надежность аппаратно-программных средств;

– недостаточный уровень организации работы системы электропитания, заземления или кондиционирования;

- умышленные угрозы, которые имеют место в следующих случаях:

– незаконное проникновение в систему злоумышленников;

– противозаконные действия обиженных пользователей.

Основными источниками угроз информационной безопасности являются:

– отказы программного и аппаратного обеспечения;

– ошибки конфигурации параметров программного обеспечения;

– случайное или умышленное нарушение правил эксплуатации системы;

– действия обслуживающего персонала, нарушающие инструкции;

– нарушение технологии обработки информации;

– внедрение в аппаратные и программные средства компонентов, не предусмотренных документацией;

– повреждение телекоммуникационных систем связи.

Выделяют следующие основные реальные способы реализации угроз:

- компьютерные вирусы и вредоносные программы, которые установлены на компьютер и действуют без разрешения пользователя;
- «маскарад» (злоумышленник действует под видом лица, обладающего полномочиями легального пользователя);
- использование устройств перехвата информации на линиях связи;
- атаки на систему типа «отказ в обслуживании запросов пользователей», при которых злоумышленник запускает очень большое число запросов к выбранному им компьютеру, обычно к серверу, и блокирует его работу.

Уязвимости ресурсов системы – это слабые места в аппаратно-программном и организационном обеспечении АСОИиУ, которые могут быть использованы для реализации угрозы информационной безопасности, например, свободный доступ сотрудников в серверную комнату;

Для оценки рисков информационной безопасности автоматизированных информационных систем (АИС) в практической деятельности используют методы как качественного, так и количественного анализа, которые рассмотрены в Приложении 2.

Оценку рисков информационной безопасности АСОИиУ обычно рекомендуется осуществлять в следующем порядке.

На *этапе 1* следует определить все ресурсы и объекты АСОИиУ, подлежащие защите, r_j $(j=1,...m)$, где m - число ресурсов и объектов, подлежащих защите.

На *этапе 2* следует определить:

- типы угроз информационной безопасности, y_i $(i=1,...n)$ и оценить вероятности их появления, так p_i $(i=1,...n)$ - вероятность появления угрозы i-го типа , где n - число типов угроз ИБ;

- уязвимые места ресурсов системы, а также вероятности уязвимости ресурсов за счет воздействия на них угроз, так $\gamma_{ij}\ (i=1,...n;\ \ j=1,...m)$ - вероятность уязвимости j -го ресурса системы за счет воздействия угроз i - го типа;

- вероятности реализации угроз по отношению к ресурсам системы, так, p_{ij} - вероятность реализации угрозы i -го типа по отношению j - му ресурсу.

$$p_{ij} = p_i \cdot \gamma_{ij} \qquad (i=1,...n;\ \ j=1,...m) \qquad (4.2)$$

При задании показателей вероятности появления угроз p_i и вероятности уязвимости ресурсов этими угрозами γ_{ij} рекомендуется использовать качественные (словесные) или количественные (бальные) оценки, как показано на примере оценки угроз в табл. 4.2. При этом уязвимость ресурса также можно оценивать качественно (малая, средняя, большая), а для перевода качественных значений в количественные значения использовать шкалу, приведенную в табл. 4.2.

Таблица 4.2

Способы оценки степени появления угрозы

Оценка степени появления угрозы		Средняя частота появления угрозы и атаки
Качественная	Количественная	
Малая (М)	1	Один раз в год
Средняя (С)	2	Один раз в четыре месяца
Большая (Б)	3	Один раз в месяц

Обычно всегда сначала применяют качественную оценку, а затем с помощью вербально-числовой шкалы (табл 4.2) переводят ее в количественный показатель.

Качественную оценку вероятности реализации угроз для ресурсов системы следует оценивать на основании данных, приведенных в табл 4.3

Степень реализации угрозы для ресурса соответствует значению, которое находится на пересечении строки, где указана степень появления угрозы, и столбца, где указана степень уязвимости ресурса этой угрозой. Например, если степень появления угрозы средняя (С), а степень уязвимости ресурса малая (М), то степень реализации угрозы по этому ресурсу будет малая (М).

Таблица 4.3

Степень реализации угроз для ресурсов системы

Степень появления угрозы	**Степень уязвимости ресурса системы**		
	Малая	**Средняя**	**Большая**
Большая	**С**	**Б**	**Б**
Средняя	**М**	**С**	**Б**
Малая	**М**	**М**	**С**

На *этапе 3* следует определить ценности ресурсов АСОИиУ.и оценить уровень их информационной безопасности и системы в целом. Ценность ресурса системы — это экономический показатель, который измеряется в суммарных денежных потерях, затрачиваемых как на восстановление системы после проникновения в нее

злоумышленника и реализацию угрозы, так и на потери, имеющие место вследствие утечки информации.

Ценность ресурса также может быть представлена также в виде качественной или количественной (бальной) оценки (аналогично табл. 4.2). Поэтому при качественной оценке ресурс может иметь малую, среднюю и большую ценность.

Далее, используя данные, приведенные в табл. 4.4, проводится оценка уровня ИБ ресурса. на качественном уровне. Уровень информационной безопасности ресурса системы соответствует значению, которое находится на пересечении строки, где указана степень реализации угрозы для ресурса, и столбца, где указана ценность этого ресурса. Например, если степень реализации угрозы для ресурса средняя (С), а ценность этого ресурса малая (М), то уровень информационной безопасности ресурса малый (М).

Таблица 4.4

Оценка уровня информационной безопасности ресурса системы

Степень реализации угрозы	**Ценность ресурса системы**		
	Малая	**Средняя**	**Большая**
Большая	**И2**	**И2**	**И1**
Средняя	**И3**	**И2**	**И2**
Малая	**И4**	**И3**	**И2**

Согласно табл. 4.4 имеют место четыре уровня информационной безопасности ресурсов системы:

уровень И1 – информационная угроза носит недопустимый характер, поэтому внедрение системы защиты информации должно быть выполнено немедленно;

уровень И2 – информационная угроза носит существенный характер, поэтому внедрение системы защиты информации должно быть выполнено в ближайшее время по мере возможности;

уровень И3 – информационная угроза носит допустимый характер, однако требуется провести мониторинг ситуации и по его результатам принять решение о целесообразности принятия мер, противодействующих угрозе, и необходимости внедрения системы защиты информации;.

уровень И4– информационная угроза несущественна, поэтому никаких действий по внедрению системы защиты информации, противодействующей данной угрозе, предпринимать пока не требуется.

Для количественной оценки риска ИБ системы (финансовых потерь) следует: определить средние ожидаемые реальные потери «c» по формуле:

$$c = \sum_{j=1}^{m} c_j = \sum_{i=1}^{n} \sum_{j=1}^{m} p_{ij}^{*} \cdot c_{ij}. \qquad (4.3)$$

Где c_j — уровень финансовых потерь из-за реализации угроз по отношению к ресурсу j-го типа;

c_{ij} — уровень финансовых потерь из-за реализации угрозы i-го типа по отношению к ресурсу j-го типа;

p_{ij}^{*} - нормированное значение вероятности реализации информационной угрозы i -го типа по отношению к j -му ресурсу .

$$p_{ij}^{*} = p_{ij} / \sum_{i=1}^{n} \sum_{j=1}^{m} p_{ij} \qquad (4,4)$$

p_{ij} — вероятность реализации угрозы *i*-го типа по отношению к *j*-му ресурсу.

- n - число типов угроз
- m число ресурсов системы

В зависимости от значения величины «с», рассчитанной по формуле (4.3), следует принимать соответствующие меры для решения проблемы обеспечения информационной безопасности АСОИиУ. Так если значение «c» составляет менее 5% финансовых потерь от максимально возможной величины ущерба, то к системе защиты, как правило, претензий нет.

Иначе, чем большую долю от максимально возможной величины ущерба составляет величина «c», тем более серьезные требования следует предъявлять к организации системы защиты информации.

На *этапе 4* следует сформировать политику информационной безопасности системы, которая представляет собой набор правил и практических рекомендаций по организации защиты информации в АСОИиУ и утверждается руководством организации.

Поскольку политика информационной безопасности определяет зоны безопасности АСОИиУ, при ее разработке необходимо соблюдать следующие принципы:

- все запросы к системе должны проходить через защитные средства;
- в системе защитных средств необходимо постоянно усиливать самое слабого звена защиты;
- пользователям предоставлять только те права доступа, которые необходимы для выполнения служебных обязанностей;
- применять многоуровневую защиту для затруднения действий как злоумышленника, так и злонамеренных или неквалифицированных действий обслуживающего персонала и пользователей;
- использовать централизованное администрирование;
- постоянно проводить практическое и теоретическое обучение обслуживающего персонала и пользователей по совершенствованию типовых мер защиты информации.

К числу основных вопросов политики информационной безопасности относятся:

- определение целей политики информационной безопасности;
- создание принципов и правил организации парольной системы защиты;
- создание инструкций по назначению привилегий для различных категорий пользователей и групп пользователей;
- разработка инструкций для пользователей по борьбе с компьютерными вирусами и другими вредоносными программами;

- установление типовых обязанностей пользователей и мер ответственности за нарушение правил работы за компьютерами;
- разработка программ обучения обслуживающего персонала и пользователей вопросам защиты информации;
- создание инструкций по ликвидации последствий нарушения информационной безопасности;
- разработка принципов и правил обновления средств защиты информации.

Разработка политики информационной безопасности завершается созданием плана обеспечения безопасности, т. е. документа, содержащего описание мер, средств и способов реализации информационной безопасности ресурсов и системы в целом, а также необходимую последовательность действий.

На *этапе 5* следует определить основные уровни обеспечения информационной безопасности АСОИиУ и все виды средств защиты, которые нужно использовать на этих уровнях. Эти вопросы подробно рассмотрены в следующем параграфе.. Здесь только отметим, что для обеспечения информационной безопасности АСОИиУ администраторы и пользователи должны строго соблюдать и выполнять следующие типовые рекомендации:

- использовать только лицензионное ПО;
- своевременно проводить автоматические обновления ОС, рекомендуемые разработчиками программных продуктов;
- не открывать неизвестные письма, полученные по электронной почте;
- осуществлять работу на компьютере в сети Интернет с ограниченными правами пользователя;

- использовать антивирусное ПО и постоянно следить за его обновлением;
- регулярно выполнять сканирование жестких дисков компьютеров в поисках вирусов;
- архивировать файлы с целью минимизации ущерба от вирусной атаки;
- при работе в сети использовать брандмауэр, позволяющий резко снизить степень проникновения на компьютер вредоносного ПО.

4.3 Организация многоуровневой защиты информации в АСОИиУ

Выделяют следующие уровни многоуровневой защиты информации в АСОИиУ и основные средства защиты, которые следует использовать на этих уровнях.

Уровень 1 — это защита серверов АСОИиУ от несанкционированного доступа. На этом уровне защиты для обеспечения доступа к серверам только легализованных пользователей администратор должен использовать парольную систему защиты, которая обычно включает поддержку следующих трех функций:

1) идентификация пользователя — процедура проверки регистрационного имени пользователя;

2) аутентификация пользователя — процедура проверки подлинности пользователя по введенному им паролю;

3) адресация пользователя — процедура проверки разрешенного по времени входа в сеть и адреса компьютера (или компьютеров), с которых разрешен вход в сеть.

Для удаленного подключения пользователя к серверу следует использовать схему возвратного звонка, которая гарантирует, что удаленный пользователь получил доступ к серверу с разрешенного номера.

Уровень 2 — это защита данных и приложений от атак злоумышленников.

На этом уровне защиты для обеспечения доступа к данным и приложениям только легализованных пользователей администратору следует использовать средства ОС, которые включают поддержку следующих двух функций:

- авторизация пользователя — процедура проверки полномочий и привилегий пользователя на предоставление ему возможности выполнять те действия, которые разрешил администратор;
- апелляция пользователя — процедура ведения и протоколирования действий, совершаемых пользователем на сервере, которые влияют на безопасность информации, расположенной на этом сервере.

Поэтому для каждого пользователя администратор должен установить индивидуальные права на доступ к файлам данных, регламентирующие все действия, которые пользователь может выполнять над этими файлами. Для каждого файла администратор также должен установить индивидуальные атрибуты, регламентирующие возможные действия с этим файлом.

Уровень 3 — это защита узлов АСОИиУ от компьютерных вирусов.

На этом уровне защиты администратору следует устанавливать антивирусные программы. Существует достаточно много программных средств антивирусной защиты. К наиболее эффективным и популярным антивирусным программам относятся Антивирус Касперского, AVAST, Norton AntiVirus.

Современные антивирусные программы состоят из модулей, которые позволяют выявить неизвестные вирусы, обновить вирусную базу данных, проверить, обнаружить и удалить фиксированный набор известных вирусов. Некоторые из этих программ включают также сетевой экран, который обеспечивает защиту компьютера от атак злоумышленников.

Администратор и пользователи должны помнить, что основными признаками наличия вирусов в компьютере являются:

- медленная загрузка и медленная работа компьютера;
- зависания и сбои в работе компьютера;
- неправильная работа ранее успешно работающих программ;
- уменьшение размера свободной области ОП;
- изменение размеров файлов и появление неизвестных файлов;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- частый вывод на экран монитора сообщений об ошибках;
- частое появление на экране монитора всплывающих меню.

Уровень 4 — это защита внутренней сети АСОИиУ от утечки информации при передаче ее между узлами сети. На этом уровне защиты администратору следует использовать специальные протоколы передачи данных, обеспечивающие конфиденциальность информации. Одним из наиболее распространенных протоколов является протокол IP Security.

Уровень 5 — это защита логического (или программного) периметра АСОИиУ от внешних атак злоумышленников за счет использования межсетевого экрана или брандмауэра. Брандмауэр (Firewail) — это компьютер с установленным на нем специальным программным обеспечением, который обеспечивает защиту системы от вторжений злоумышленников из глобальной сети, позволяет пропускать через сетевое подключение системы только авторизованный трафик и осуществляет протоколирование всех событий. Он также может осуществлять шифрование информации, обеспечивать только ее одностороннюю передачу и блокировать нежелательную активность внешнего трафика.

Отметим следующие основные недостатки брандмауэра:

– он обеспечивает эффективную защиту логического периметра АСОИиУ только при очень точной настройке его рабочих параметров, что требует большого опыта работы администратора;

– он не обеспечивает защиту АСОИиУ от атак, выполняемых изнутри системы, например, «обиженными» пользователями».

Уровень 6 — это защита физического периметра АСОИиУ в результате ограничения доступа персонала в помещения, в которых расположены ресурсы системы. Обслуживающий персонал и пользователи должны иметь право посещать только помещения, выделенные им для выполнения служебных обязанностей.

Поскольку важную роль в организации информационной безопасности АСОИиУ играет парольная система защиты, которую разрабатывает и устанавливает администратор системы, рассмотрим ее более подробно.

Парольную систему защиты сервера АСОИиУ Y можно представить в виде следующего набора параметров:

$$Y = (L,\ A,\ T,\ N,\ S,\ B,\ R), \qquad (4.5)$$

где L — длина пароля, т. е. число символов в составе пароля; A — мощность алфавита пароля, т.е. количество символов, которые могут входить в состав пароля; T — срок действия пароля, т. е. периодичность изменения пароля; N — уникальность пароля, т. е. его повторяемость, определяет сколько раз новый пароль не должен повторять старый, или через сколько

паролей новый пароль может повторить старый пароль; S — число входов в систему со старым просроченным паролем после истечения срока его действия; B — блокировка пароля после неверного его ввода, которая указывает, сколько раз последовательно друг за другом пользователь может неверно набрать и ввести пароль; R — режим разблокирования пароля, который указывает, через какой промежуток времени и какими средствами возможно провести разблокирование пароля для обеспечения подключения легального пользователя к сети.

Вероятность P подбора злоумышленником пароля легального пользователя сети в течение срока действия этого пароля определяется согласно выражению

$$P = \frac{vT}{W}, \tag{4.6}$$

где v — скорость подбора пароля пользователя злоумышленником; T — срок действия пароля пользователя; W — мощность пространства паролей,

$$W = A^L \tag{4.7}$$

(A — мощность алфавита пароля; L — длина пароля пользователя).

После подстановки выражения (4.7) в (4.6) получаем

$$P = \frac{vT}{A^L}. \tag{4.8}$$

После преобразования выражения (4.8) получаем

$$A^L = \frac{vT}{P}. \tag{4.9}$$

В результате дальнейшего преобразования выражения (4.9) получаем выражение для определения требуемой длины пароля пользователя в зависимости от срока его действия, скорости и вероятности подбора пароля злоумышленником и мощности алфавита пароля, которое имеет вид

$$L = \frac{\ln(vT/P)}{\ln A}. \tag{4.10}$$

При задании мощности алфавита пароля A администратор должен учитывать особенности клавиатуры компьютера, принципы работы пользователя за этой клавиатурой, а также требования сетевой ОС. Поэтому администратору рекомендуют использовать следующие способы задания мощности алфавита пароля:

- $A = 36$, если для набора символов, входящих в состав пароля, используются буквы латинского алфавита без изменения регистра и цифры от 0 до 9;

- $A = 62$, если для набора символов, входящих в состав пароля, используются буквы латинского алфавита верхнего и нижнего регистров, а также цифры от 0 до 9.

Для задания остальных исходных, входящих в состав выражения (9.8) и необходимых для определения требуемой длины пароля пользователя АСОИиУ, администратору рекомендуют использовать следующие значения:

- срок действия пароля — один месяц, т. е. T = 30 сут = 720 ч = = 2,592 10^6 с;
- скорость подбора пароля пользователя злоумышленником с использованием современных компьютеров при отсутствии режима блокировки пароля изменяется в пределах от $v = 10^5$ до $v = 10^7$ паролей/с;
- вероятность подбора злоумышленником пароля администратора — не более 10^{-12}, пользователя, решающего важные задачи, — не более 10^{-10}, а обычного пользователя — не более 10^{-8}.

Результаты расчетов, проведенных с использованием выражения (4.10) при подстановке в него рекомендуемых числовых значений исходных данных без использования режима блокировки ввода пароля, приведены в табл. 4.5

Таблица 4.5

Выбор длины пароля

Вероятность подбора пароля P	Длина пароля L					
	A = 36			A = 62		
	$v = 10^5$	$v = 10^6$	$v = 10^7$	$v = 10^5$	$v = 10^6$	$v = 10^7$
10^{-15}	16,98	17,63	18,28	14,72	15,29	15,84
10^{-14}	16,35	16,98	17,63	14,17	14,72	15,29
10^{-13}	15,70	16,35	16,98	13,61	14,17	14,72
10^{-12}	15,06	15,70	16,35	13,06	13,61	14,17
10^{-11}	14,43	15,06	15,70	12,50	13,06	13,61
10^{-10}	13,77	14,43	15,06	11,94	12,50	13,06
10^{-9}	13,13	13,77	14,43	11,38	11,94	12,50
10^{-8}	12,43	13,13	13,77	10,82	11,38	11,94
10^{-7}	11,84	12,43	13,13	10,28	10,82	11,38
10^{-6}	11,20	11,84	12,43	9,72	10,28	10,82
10^{-5}	10,56	11,20	11,84	9,15	9,72	10,28

При использовании режима автоматической блокировки ввода пароля в случае нескольких n последовательных неверных попыток ввода пароля ОС будет автоматически осуществлять блокировку его дальнейшего ввода на некоторый промежуток времени $T_{бл}$. Скорость подбора злоумышленником пароля пользователя $v_{бл}$ при наличии блокировки существенно снижается по сравнению с ее отсутствием и определяется из выражени

$$v_{\text{бл}} = \frac{n}{T_{\text{бл}}}. \qquad (4.11)$$

Типовые значения времени блокировки ввода пароля пользователя и скорости подбора пароля, вычисленные по выражению (4.11), при числе неверных попыток ввода пароля $n = 3$, которое наиболее широко используют администраторы в их практической работе, приведены в табл. 4.6.

Таблица 4.6

Связь времени блокировки и скорости подбора пароля

Время блокировки ввода пароля, устанавливаемое администратором сети, мин	$T_{\text{бл}}$, с	Скорость подбора пароля при наличии блокировки $v_{\text{бл}}$, паролей/с
15	900	0,003333
5	300	0,01
1	60	0,05

При использовании режима автоматической блокировки ввода пароля выражение для определения требуемой длины пароля пользователя с учетом выражений (4.10) и (4.11) имеет вид

$$L_{\text{бл}} = \frac{\left(\ln \frac{v_{\text{бл}} T}{P}\right)}{\ln A}, \qquad (4.12)$$

где $L_{\text{бл}}$ — длина пароля пользователя при наличии режима блокировки ввода пароля.

При этом количество символов ΔL, на которое уменьшается длина пароля при его блокировке, можно определить из выражения

$$\Delta L = L - L_{\text{бл}} = \frac{\left(\ln \frac{vT}{P}\right)}{\ln A} - \frac{\left(\ln \frac{v_{\text{бл}} T}{P}\right)}{\ln A} = \frac{\left(\ln \frac{v}{v_{\text{бл}}}\right)}{\ln A}. \qquad (4.13)$$

При расчетах $\ln A$ принимает следующие значения: $\ln 36 = 3{,}58$ и $\ln 62 = 4{,}13$. Исходные данные для расчета $\left(A,\ v,\ v_{\text{бл}}\right)$, а также значения ΔL, вычисленные по выражению (4.13), приведены в табл. 4.7

Таблица 4.7

Уменьшение длины пароля за счет использования режима блокировки

$v_{\text{бл}}$, паролей/с	Уменьшение длины пароля ΔL при использовании режима блокировки пароля					
	A = 36			A = 62		
	$v = 10^5$	$v = 10^6$	$v = 10^7$	$v = 10^5$	$v = 10^6$	$v = 10^7$
0,003333	4,80	5,45	6,10	4,16	4,73	5,28
0,01	4,50	5,15	5,79	3,92	4,46	5,02
0,05	4,05	4,70	5,34	3,51	4,07	4,63

Анализ результатов, приведенных в табл. 4.7, показывает, что использование режима блокировки ввода пароля пользователя позволяет уменьшить длину пароля пользователя на 4–5 символов, обеспечивая надлежащий уровень защиты сервера от проникновения на него злоумышленников.

Следует дать основные рекомендации администратору по формированию парольной системы защиты сервера:

1) на сервере ЛВС целесообразно установить режим автоматической блокировки ввода пароля пользователя, при котором после трех неверных попыток подключения пользователя к серверу вход в сеть блокируется на время, равное одной минуте;

2) пароль пользователя не должен содержать осмысленных слов из словаря, чтобы резко уменьшить скорость его подбора;

3) пароль пользователя не должен представлять собой слово, которое часто употребляет пользователь;

4) пароль пользователя должен соответствовать алфавиту $A = 62$ и содержать символы верхнего и нижнего регистров кла-виатуры компьютера;

5) пароль пользователя должен содержать не менее 7 символов, включать строчные и прописные буквы, а также цифры;

6) пароль пользователя должен иметь ограниченный срок действия, но не более 30 сут;

7) пароль пользователя должен быть составлен таким образом, чтобы достаточно просто и легко было запомнить метод его получения, а по возможности — и сам пароль.

Контрольные вопросы и задания к главе 4

1. Перечислите основополагающие документы по защите информации в Российской Федерации
2. Поясните назначение Доктрины информационной безопасности РФ
3. Перечислите уровни правового обеспечения защиты информации и документы, соответствующие этим уровням.
4. Перечислите документы, которые входят в систему стандартов информационной безопасности
5. Поясните назначение документа «Оранжевая книга».
6. Что составляет сходство и в чем различие документов «Критерии оценки безопасности информационных технологий» и «Общие критерии оценки безопасности информационных технологий».
7. Поясните различие между документами «Оранжевая книга» и «Общие критерии оценки безопасности информационных технологий».
8. Поясните назначение групп и классов, изложенных в документе по защите информации от несанкционированного доступа, разработанном Гостехкоммисией России.
9. Поясните понятие защита информации.
10. Что такое информационная безопасность АСОИиУ?
11. Приведите выражения для оценки меры уязвимости ресурса АСОИиУ.
12. Перечислите этапы организации информационной безопасности АСОИиУ.
13.. Поясните назначение уровней защиты информации в АСОИиУ.
14. Перечислите средства, которые следует использовать администратору при защите информации в АСОИиУ?
15. Приведите правила формирования парольной системы защиты сервера.

Литература к главе 4

Основная

Баранова Е.К. Информационная безопасность и защита информации: учеб. пособие. / Е.К. Баранова, А.В. Бабаш. М.: РИОР ИНФРА-М, 2014. 256 с.

Дополнительная

Жук А.П.. Защита информации: учеб. пособие../ А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. М.: РИОР, ИНФРА- М, 2011. 392 с.

Глава 5. Выбор вариантов развития АСОИиУ на основе аналитических методов

5.1 Выбор перспективного направления развития АСОИиУ на основе метода сбалансированного решения

Метод сбалансированного решения довольно часто используют при выборе перспективного направления развития АСОИиУ в условиях полной неопределенности, когда эффективность выбранного варианта развития АСОИиУ существенно зависит от условий окружающей среды, которые заранее не известны. Известна лишь матрица доходов, строки которой соответствуют возможным условиям проявления внешней среды, а столбцы – возможным вариантам развития АСОИиУ.

Каждый элемент a_{ij} этой матрицы – это доход, который имеет место при этом i - ом ($i=1,..n$) условии внешней среды и j -ом $j=1,..m$ варианте развития АСОИиУ. При этом

n - число рассматриваемых условий внешней среды

m - число рассматриваемых вариантов развития АСОИиУ

Этот метод позволяет в качестве наилучшего варианта - B_l развития АСОИиУ, выбрать такой вариант, из набора рассматриваемых альтернативных вариантов, для которого значение критерия максимально. Критерий сбалансированного решения имеет следующий вид:

$$B_l = \max_j B_j = \max_j \left[\; a_1 \max_i a_{ij} + a_2 \min_i ac_{ij} + a_3 \frac{1}{n} \sum_{i=1}^{n} a_{ij} \; \right] \qquad (5.1)$$

При этом обязательно должны быть выполнены следующие условия

$$\sum_{i=1}^{3} a_i = 1 \quad \text{и} \quad 0 \le a_i \le 1$$

Где a_1 , a_2 , a_3 - соответственно коэффициенты оптимизма, пессимизма и реализма, рекомендуемые значения которых $a_1 = a_2 = a_3 = 1/3$

Из этого критерия, при определенных значениях коэффициентов a_i , можно получить широко используемые на практике частные типовые критерии принятия решения в условиях полной неопределенности, которые приведены в таб. 5.1

Таблица 5.1

Значения коэффициентов оптимизма, пессимизма и реализма при которых, из сбалансированного критерия, получают типовые критерии для принятия решения в условиях полной неопределенности.

№	Значения коэффициентов сбалансированного критерия	Название критерия
1	$a_1 = 1/3 \quad a_2 = 1/3 \quad a_3 = 1/3$	Критерий сбалансированного решения
2	$a_1 = 0 \quad a_2 = 0 \quad a_3 = 1$	Критерий Лапласа
3	$a_1 = 1 \quad a_2 = 0 \quad a_3 = 0$	Критерий максимаксимума
3	$a_1 = 0 \quad a_2 = 1 \quad a_3 = 0$	Критерий Вальда
4	$a_1 + a_2 = 1 \quad a_3 = 0$	Критерий Гурвица
5	$a_1 = 0 \quad a_2 + a_3 = 1$	Критерий Ходжа-Лемана

Критерии, приведенные в табл. 5.1 , имеют следующий смысл:

1. критерий сбалансированного решения – это критерий взвешенного оптимизма, пессимизма и реализма, позволяет выбрать рациональный вариант развития АСОИиУ;
2. критерий Лапласа – это критерий реализма, который предполагает, что все возможные состояния будущей природы равновероятны и позволяет выбрать такой вариант развития АСОИиУ, для которого значение среднего дохода с учетом всех возможных состояний внешней среды принимает максимальное значение.
3. критерий максимаксимума - это критерий "крайнего оптимизма", предполагает выбор такого развития АСОИиУ, который дает нам самый большой доход без учета реального состояния будущей внешней среды.
4. критерий Вальда – это критерий "крайнего пессимизма", так как предполагает выбор такого варианта развития АСОИиУ, который дает нам самый большой доход в самых неблагоприятных для нас условиях, т.е выбирается вариант, который имеет максимальный минимальный доход среди сравниваемых вариантов.
5. критерий Гурвица – это критерий взвешенного оптимизма-пессимизма, который учитывает мнение как оптимиста, так и пессимиста.

При $a_1 = 1,\ a_2 = 0,\ a_3 = 0$ имеет место ситуация крайнего оптимизма и критерий сводится к критерию максимакса

При $a_1 = 0,\ a_2 = 1,\ a_3 = 0$ имеет место ситуация крайнего пессимизма и критерий сводится к критерию Вальда,т.е. максимина.

На практике, в случае полной неопределенности, рекомендуется использовать значения $a_1 = a_2 = 0{,}5$ и $a_3 = 0$

6. критерий Ходжа-Лемана – это критерий взвешенного реализма-пессимизма, учитывает мнение, как реалиста, так и пессимиста.

если $a_1 = 0,\ a_2 = 0,\ a_3 = 1$, то критерий превращается в критерий Лапласа;

если $a_1 = 0,\ a_2 = 1,\ a_3 = 0$, то критерий превращается в критерий Вальда

На практике, в случае полной неопределенности, рекомендуется использовать значения $a_1 = 0$ и $a_2 = a_3 = 0{,}5$

Пример 5.1 Руководство фирмы поставило перед аналитическим отделом задачу определить целесообразность проведения модернизации или реорганизации организационной структуры и архитектуры системы обработки информации, размещенной в главном офисе этой фирмы. При этом необходимо рассмотреть и сравнить четыре варианта решения:

Вариант 1 - (В1) - оставить организационную структуру и архитектуру системы без изменения;

Вариант 2 – (В2) - провести модернизацию архитектуры системы;

Вариант 3 – (В3) – провести реорганизацию организационной структуры и архитектуры системы;

Вариант 4 – (В4) - провести реорганизацию организационной структуры.

При выборе варианта решения следует учесть возможные состояния (условия) окружающей среды, т.е. будущей внешней среды, которая существенно влияет на количество клиентов фирмы и ее доходы.

Условие 1 – (У1) -. обстановка, окружающая фирму, не изменяется;

Условие 2 – (У2) - вблизи фирмы возможен ввод в действие филиала конкурирующей фирмы;

Условие 3 – (У3) - вблизи фирмы возможно строительство жилого массива;

Условие 4 – (У4) - вблизи фирмы возможен ввод в действие филиала конкурирующей фирмы; а также строительство жилого массива.

Расчеты, проведенные экономистами фирмы, позволили получить матрицу средних возможных доходов фирмы, для рассматриваемых вариантов реорганизации системы при возможных вариантах окружающей среды, которая приведена в табл. 5.2.

Необходимо провести ранжирование исходных вариантов по степени их предпочтительности и выбрать направление развития АСОИиУ, т. е. наилучший вариант развития из рассматриваемых вариантов.

Таблица 5.2

Матрица доходов фирмы

Условие внешней среды	Доход фирмы от возможного варианта построения организационной структуры и архитектуры системы обработки информации			
	Вариант 1	Вариант 2	Вариант 3	Вариант 4
Условие 1	10	9	8	6
Условие 2	8	5	6	4
Условие 3	14	16	18	20
Условие 4	12	13	14	12

Решение. Расчеты, проведенные по методу сбалансированного критерия с использованием выражения (5.1), приведены в табл. 5.3. Коэффициенты, оптимизма a_1, пессимизма a_2 и реализма a_3 имеют значения. $a_1 = a_2 = a_3 = 1/3$, что соответствует режиму сбалансированного решения

Таблица 5.3

Выбор варианта решения по критерию сбалансированного решения

Условия внешней среды	Возможные варианты решения			
	B1	B2	B3	B4
Условие 1	10	9	8	6
Условие 2	8	5	6	4
Условие 3	14	16	18	20
Условие 4	12	13	14	12
$B_{j1} = \alpha_1 \max_i a_{ij}$	4,667	5,333	6	6,667
$B_{j2} = \alpha_2 \min_i a_{ij}$	2,667	1,667	2	1,333
$B_{j3} = \alpha_3 \frac{1}{n} \sum_{i=1}^{n} a_{ij}$	3,667	3,583	3,833	3,5
$B_j = (B_{j1} + B_{j2} + B_{j3})$	11	10,583	11,833	11,5
$B = \max_j B_j$			11,833 (*)	

Примечание. Знаком (*) отмечен лучший вариант решения

Анализ результатов, приведенных в табл. 5.3 , показывает, что наилучшим вариантом развития АСОИиУ по методу сбалансированного решения, в условиях полной неопределенности, является вариант B3. Ранжирование вариантов по степени предпочтения имеет вид: $B3 \succ B4 \succ B1 \succ B2$

5.2 Выбор стратегического плана развития АСОИиУ на основе метода «дерева целей»

Метод «дерева целей» позволяет получить, стратегическую последовательность выполнения отдельных мероприятий, способствующих совершенствованию АСОИиУ и достижению глобальной цели ее развития.

Этот метод известен также как метод Паттерн (PATTERN – Planning Assistance Through Technical Relevance Number) - это помощь в проведении планирования при сравнении альтернативных вариантов развития системы за счет использования относительных показателей технической оценки.

Метод «дерева целей» включает следующие этапы:

Этап 1 Формирование глобальной цели и написание подробного древовидного сценария частных целей для ее достижения, т.е. определение набора возможных вариантов для решения проблемы.

Этап 2 Построение «дерева целей» за счет использования принципа иерархии целей Идея этого принципа состоит в том, что любая цель более высокого уровня преобразуется в совокупность целей более низкого уровня., т.е. каждая крупная цель разбивается на более мелкие цели. Таким образом, все сформированные цели выстраиваются в иерархический ряд с учетом их строгой логической последовательности.

Процесс построения «дерева целей» включает следующие шаги:

- формулировка глобальной цели;
- формирование уровней иерархии «дерева целей», когда выполняется генерация промежуточных и конечных (т.е. локальных) целей; при этом на каждом уровне иерархии обязательно должно быть несколько целей;
- уточнение и корректировка формулировок промежуточных и конечных целей с учетом выполнения принципа их реализуемости;
- построение связей между глобальной, промежуточными и конечными целями.
- оценка уровня важности всех целей, входящих в состав «дерева целей».

При построении «дерева целей» следует выполнять следующие правила:

- все дерево целей представляет собой единую цель системы;
- каждая цель должна иметь свой уникальный номер в «дереве целей», а также средства и ресурсы для ее обеспечения;
- декомпозиция каждой цели верхнего уровня на цели нижнего уровня осуществляется по одному выбранному классификационному признаку;

- количество целей нижнего уровня должно быть достаточным для достижения цели верхнего уровня;

- по мере перехода от целей верхнего уровня к целям нижнего уровня эти цели приобретают все более конкретный характер;

- развитие отдельных ветвей дерева может заканчиваться на разных уровнях иерархии «дерева целей»;

- вершины вышележащего уровня «дерева целей» представляют собой цели для вершин нижележащих уровней;

- построение «дерева целей» продолжается до тех пор, пока лицо принимающее решение не будет иметь в своем распоряжении все конечные, т.е. все локальные, цели для достижения вышестоящей глобальной цели.

Этап 3. Формирование группы критериев для оценки относительной важности, полезности, экономической эффективности целей всех уровней. При этом также проводится оценка и относительной важности всех этих критериев. Составляются сводные таблицы для промежуточных и локальных целей одного уровня «дерева целей», относящихся к одному и тому же вышестоящему уровню целей.

Далее будем использовать следующие обозначения: и выражения для оценки эффективности использования промежуточных и локальных целей при достижении глобальной цели.

$\alpha_k^{(i)}$ - вес k-го критерия, относящегося к цели, которая является целью более низкого уровня по отношению к цели, имеющей i-ый номер в иерархии целей, и непосредственно с ней связана.

$S_{jk}^{(i)}$ - коэффициент относительного веса цели по k-му критерию, имеющей j- ый номер в иерархии целей и непосредственно связанной с целью, имеющий i-ый номер,

При этом обязательно должны быть выполнены следующие условия:

1) сумма весовых коэффициентов критериев, относящихся к одному уровню иерархии «дерева целей», который непосредственно связан с одним вышестоящим уровнем этого дерева должна быть равна единице.

$$\sum_{k=1}^{n_i} \alpha_k^{(i)} = 1 \qquad \text{для} \quad i = const \tag{5.2}$$

где n_i - количество критериев, которое следует учитывать при анализе целей, которые являются целями более низкого уровня по отношению к цели, имеющей i -ый номер в иерархии целей, с которой они непосредственно связаны.

2) сумма коэффициентов относительных весов целей, расположенных на i-ом уровне иерархии «дерева целей», который связан с одним вышестоящим уровнем этого дерева должна быть также равна единице.

$$\sum_{j=1}^{n_j} S_{jk}^{(i)}=1 \qquad \text{для} \quad i = const \qquad (5.3)$$

где n_j - количество целей,, которые являются целями более низкого уровня по отношению к цели, имеющей i -ый номер в иерархии целей, с которой они непосредственно связаны.

Далее по формуле (5.4) вычисляем $r_j^{(i)}$ - коэффициент относительного веса цели, имеющей j - ый номер в иерархии целей и непосредственно связанной с целью, имеющий i -ый номер.

$$r_j^{(i)} = \sum_{k=1}^{n_i} \alpha_k^{(i)} \cdot S_{jk}^{(i)} \qquad (5.4)$$

В многоуровневой иерархической структуре рассмотренная процедура повторяется на каждом уровне для каждого узла» «дерева целей». При этом каждый узел этого дерева соответствует промежуточной или локальной цели и поэтому имеет свой индивидуальный номер в дереве иерархии целей..

Процедуру оценки, как правило, начинают с самого верхнего уровня «дерева целей», перемещаясь каждый раз на уровень ниже, после проведения всех расчетов на данном уровне. Для получения значения коэффициента относительной важности каждой промежуточной или локальной цели, необходимо вычислить по формуле (5.4) соответствующее значение $r_j^{(i)}$. При этом R_j - полный к коэффициент относительной важности локальной цели, имеющей j -ый номер в иерархии целей , определяется из следующего выражения

$$R_j = \prod_{i,j \in L} r_j^{(i)} \qquad (5.5)$$

где i и j – номера целей, которые расположены на пути перемещения от главной цели, т.е. цели с номером нуль, к локальной цели с номером j.

Далее можно провести ранжирование локальных целей по показателю R_j, чем больше значение этого показателя, тем локальная цель является более важной и требует ее реализации в первую очередь. При этом самой важной локальной целью является та цель (е), для которой значение этого показателя принимает наибольшее значение согласно выражения (5.6)

$$R_e = \max_j R_j \qquad (5.6)$$

Пример 5.2 Компьютерной фирме для дальнейшего развития бизнеса, удовлетворения постоянно растущих потребностей клиентов, увеличения уровня престижа в борьбе с конкурентами необходимо разработать план развития своего центрального офиса, основу которого составляет АСОИиУ.

Главная цель фирмы (цель №0) – это эффективное развитие бизнеса за счет качественного удовлетворения постоянно растущих потребностей клиентов Руководство фирмы считает, что эту цель можно достигнуть несколькими путями, выбирает при этом в качестве основных путей, следующие два направления, т.е. две промежуточные цели

Цель №1 – Провести модернизацию аппаратно-программных средств

Цель №2 - Провести реорганизацию организационной структуры

В свою очередь промежуточная цель №1 может быть реализована с помощью следующих локальных целей:

Цель №3 – Установить более мощный сервер.

Цель №4 – Установить более современные версии ПО.

Цель №5 - Заменить кабельную систему, перейти с НВП на ВОЛС.

Промежуточная цель №2 может быть реализована с помощью следующих локальных целей:

Цель №6 - Сменить провайдера Интернет услуг

Цель №7 - Организовать службу ремонта и обслуживания компьютеров

Решение. Исходные данные для промежуточных и локальных целей, которые получены в результате проведения экспертного опроса с учетом выполнения условий (5.2) и (5.3) приведены в табл. 5.4 - 5.6

Таблица 5.4

Исходные данные и оценка коэффициентов относительного веса локальных целей №1 и №2.

Критерии	Весовой коэффициент	Цель №1	Цель №2
Рост количества клиентов	$\alpha_1^{(0)} = 0,6$	$S_{11}^{(0)} = 0,45$	$S_{21}^{(0)} = 0,55$
Рост доходов	$\alpha_2^{(0)} = 0,4$	$S_{12}^{(0)} = 0,4$	$S_{22}^{(0)} = 0,6$
$r_j^{(0)} = \sum_{k=1}^{2} \alpha_k^{(0)} \cdot S_{jk}^{(0)}$		$r_1^{(0)} = 0,43$	$r_2^{(0)} = 0,57$

Таблица 5.5

Исходные данные и оценка коэффициентов относительного веса локальных целей №3, №4 и №5

Критерии	Весовой коэффициент	Цель №3	Цель №4	Цель №5
Качество работы системы	$\alpha_1^{(1)} = 0,5$	$S_{31}^{(1)} = 0,3$	$S_{41}^{(1)} = 0,2$	$S_{51}^{(1)} = 0,5$
Престижность фирмы	$\alpha_2^{(1)} = 0,5$	$S_{32}^{(1)} = 0,2$	$S_{42}^{(1)} = 0,2$	$S_{52}^{(1)} = 0,6$
$r_j^{(1)} = \sum_{k=1}^{2} \alpha_k^{(1)} \cdot S_{jk}^{(1)}$	-	$r_3^{(1)} = 0,25$	$r_4^{(1)} = 0,20$	$r_5^{(1)} = 0,55$

Таблица 5.6

Исходные данные и оценка коэффициентов относительного веса локальных целей №6 и №7

Критерии	Весовой коэффициент	Цель №6	Цель №7
Простота проведения реорганизации	$\alpha_1^{(2)} = 0,2$	$S_{61}^{(2)} = 0,8$	$S_{71}^{(2)} = 0,2$
Объем услуг	$\alpha_2^{(2)} = 0,5$	$S_{62}^{(2)} = 0,4$	$S_{72}^{(2)} = 0,6$
Режим работы	$\alpha_3^{(2)} = 0,3$	$S_{63}^{(2)} = 0,8$	$S_{73}^{(2)} = 0,2$
$r_j^{(2)} = \sum_{k=1}^{2} \alpha_k^{(2)} \cdot S_{jk}^{(2)}$	-	$r_6^{(2)} = 0,6$	$r_7^{(2)} = 0,4$

В табл. 5.4 – 5.6 также приведены оценки коэффициентов относительного веса промежуточных и локальных целей, рассчитанные по выражению (5.4)

Полные значения коэффициентов относительной важности промежуточных целей 1 и 2, рассчитанные с использованием выражения (5.5) имеют вид: $R_1 = r_1^{(0)} = 0,43$

$R_2 = r_2^{(0)} = 0,57$

Ранжирование промежуточных целей по показателю R_j позволяет утверждать, что для достижения главной цели, а именно эффективного развития бизнеса фирмы, реорганизация организационной структуры фирмы является более перспективной задачей по сравнению с реорганизацией аппаратно-программных средств, поскольку рассчитанное значение $R_2 > R_1$

Полные значения коэффициентов относительной важности локальных целей, рассчитанные с использованием выражения (5.5), приведены ниже

$$R_3 = r_3^{(1)} \cdot r_1^{(0)} = 0,25 \cdot 0,43 = 0,1075 \qquad R_4 = r_4^{(1)} \cdot r_1^{(0)} = 0,20 \cdot 0,43 = 0,0860$$

$$R_5 = r_5^{(1)} \cdot r_1^{(0)} = 0,55 \cdot 0,43 = 0,2365 \qquad R_6 = r_6^{(2)} \cdot r_2^{(0)} = 0,6 \cdot 0,57 = 0,3420$$

$$R_7 = r_7^{(2)} \cdot r_2^{(0)} = 0,4 \cdot 0,57 = 0,2280$$

Используя выражение (5.6), получаем, что самой важной локальной целью, которую следует реализовать в первую очередь, является цель №6.

Ранжирование локальных целей по показателю R_j позволяет расположить эти цели, начиная с самой важной цели, в следующей последовательности Цель №6 – Цель №5 – Цель №7 – Цель №3 – Цель №4

Таким образом, для достижения главной цели – эффективного развития бизнеса руководство фирмы должно последовательно и поэтапно провести следующие мероприятия:

- сменить провайдера Интернет услуг (цель№6);
- заменить кабельную систему, перейти с НВП на ВОЛС.(цель №5);
- организовать службу ремонта и обслуживания компьютеров (цель №7)
- установить более мощный сервер (цель №3);
- установить более современные версии ПО (цель №4).

5.3 Выбор организационно-управленческих решений при модернизации АСОИиУ на основе метода анализа иерархий

Метод анализа иерархий или аналитической иерархии (Analytic Hierarchy Process) разработан американским ученым, математиком Томасом Саати, и научно обоснован. Метод является универсальным, достаточно мощным и эффективным средством принятия наилучших решений при решении многокритериальных задач и поэтому в настоящее время нашел широкое практическое применение. Рассмотрим основные этапы процесса принятия организационно-управленческих решений с использованием метода анализа иерархий

Этап 1 Структуризация процесса принятия решения. На этом этапе ЛПР разрабатывает иерархическую многоуровневую структурную схему процесса принятия решения и определяет основные факторы, которые входят в ее состав. К их числу относятся: главная цель исследования, критерии и набор альтернативных вариантов, подлежащих сравнению.

При этом все критерии представляют собой факторы одного типа, а все исходные альтернативные варианты сравнения – это факторы другого типа.

Этап 2 Последовательное парное сравнение всех факторов одного типа. На этом этапе ЛПР выполняет следующие действия:

1. Составляет матрицу парных сравнений критериев, в которую заносит результаты сравнения всех критериев,

При сравнении любых двух критериев ЛПР сначала должен указать в словесной формулировке какой из этих критериев является более важным. Для измерения степени превосходства одного критерия перед другим ЛПР использует логические суждения из упрощенной или фундаментальной вербально-цифровых шкал, соответственно приведенных в табл 5.7 и табл 5.8, а затем переводит эти данные в числа k_{ij}, согласно этим же шкалам.

Если в матрице парных сравнений критерий строки (i) имеет степень предпочтительности по сравнению с критерием столбца (j), то в соответствующий элемент матрицы записываем число k_{ij}, тогда элемент на пересечении строки (j) и столбца (i) будет иметь обратное значение, равное $1/k_{ij}$.

Таблица 5.7

Вербально-числовая шкала относительной предпочтительности показателей, предложенная Саати

№	Качественное определение уровня предпочтительности	Количественное значение уровня предпочтительности (k_{ij})
1	Равная предпочтительность	1
2	Умеренная степень предпочтительности	3
3	Существенная степень предпочтительности	5
4	Значительная степень предпочтительности	7
5	Очень большая степень предпочтительности	9

Числа 2,4,6,8 используются для оценки промежуточных значений

Таблица 5.8

Фундаментальная вербально- числовая шкала относительной предпочтительности показателей, предложенная Саати

№	Качественное определение уровня предпочтительности	Количественное значение уровня предпочтительности (k_{ij})
1	Равная предпочтительность	1
2	Слабая степень предпочтительности	2
3	Среднее степень предпочтительности	3
4	Предпочтительность выше среднего	4
5	Умеренно сильная предпочтительность	5
6	Сильная предпочтительность.	6
7	Очень сильная (очевидная) предпочтительность	7
8	Очень, очень сильная предпочтительность	8
9	Абсолютная предпочтительность	9

Если количество критериев равно (n), то количество парных сравнений критериев определяется из следующего выражения $\left[\; n \cdot (n-1)/2 \; \right]$

2. После заполнения матрицы парных сравнений критериев ЛПР составляет матрицы парных сравнений исходных альтернативных вариантов по каждому из критериев. Если количество вариантов сравнения равно m, то количество парных сравнений вариантов по всем критериям определяется из выражения

$\left[\; n \cdot m \cdot (m-1)/2 \; \right]$

Процедура парного сравнения исходных вариантов по каждому критерию аналогична процедуре сравнения критериев друг с другом.

Следует иметь в виду, что любая матрица парных сравнений факторов, составленная ЛПР, должна обладать следующими свойствами:

1) быть квадратной и положительной;

2) все элементы главной диагонали матрицы должны быть равны единице;

3) любые два элемента матрицы парных сравнений ,симметричные относительно ее главной диагонали, должны быть связаны между собой следующим соотношением $k_{ij} = 1/k_{ji}$, которое следует из основного правила заполнения матрицы;

4) для любых элементов k_{ik} , k_{ij} , k_{jk} матрицы парных сравнений должно выполняться условие согласованности элементов, которое имеет следующий вид: $k_{ik} = k_{ij} \cdot k_{jk}$

5) для любых элементов k_{ik} , k_{ij} , k_{jk} матрицы парных сравнений должны выполняться условия транзитивности элементов, согласно которым, если $k_{ik} \geq k_{ij}$ и $k_{ij} \geq k_{jk}$, то $k_{ik} \geq k_{jk}$

Матрицу парных сравнений факторов, удовлетворяющую всем перечисленным свойствам, называют согласованной.

Этап 3 Вычисление коэффициентов важности факторов. На этом этапе ЛПР сначала вычисляет коэффициенты важности критериев, а затем коэффициенты важности исходных вариантов по каждому из этих критериев.

Для этого ЛПР последовательно вычисляет собственные вектора как критериев C_i , так и каждого исходного варианта (j) по каждому критерию (i) , т.е. C_{ij} , по следующим выражениям

$$C_i = (k_{i1} \cdot k_{i2} \cdots k_{in})^{1/n} \qquad (5.7)$$

$$C_{ij} = (k_{ij1} \cdot k_{ij2} \cdots k_{ijm})^{1/m} \qquad (5.8)$$

Всего вычисляется $\left[\; n \cdot (m+1) \; \right]$ значений собственных векторов

Далее ЛПР выполняет нормирование значений собственных векторов всех факторов и определяет коэффициенты важности (или весовые коэффициенты) этих факторов по следующим выражениям

$$\alpha_i = \frac{C_i}{\sum_{i=1}^{n} C_i} \qquad (5.9)$$

$$\beta_{ij} = \frac{C_{ji}}{\sum_{i=1}^{m} C_{ij}} \qquad (5.10)$$

где α_i - весовой коэффициент i -го критерия

β_{ij} - весовой коэффициент j -го варианта по i -му критерию

Этап 4 Определение наилучшего варианта решения Выбор наилучшего варианта решения ЛПР осуществляет в следующей последовательности:

- вычисляет показатель качества Y_j каждого j-го варианта решения ($j = 1,...m$,), используя следующее выражение

$$Y_j = \sum_{i=1}^{n} \alpha_i \cdot \beta_{ij} \qquad \text{где} \quad j = 1,....m \qquad (5.11)$$

- выбирает вариант решения (l) , для которого показатель качества Y_l принимает максимальное значение, и считает этот вариант решения наилучшим среди сравниваемых..

$$Y_l = \max_j Y_j \qquad \text{где} \quad j = 1,....m \qquad (5.12)$$

Этап 5 Проверка согласованности суждений ЛПР. На практике действия ЛПР при построении матриц парного сравнения факторов, как правило, далеки от проведения идеальных сравнений и выполнения условий согласованности и транзитивности элементов этих матриц. Эти нарушения во многом объясняются психологическими особенностями ЛПР, имеющими место при проведении им большого количества парных сравнений. Поэтому каждая матрица парных сравнений после ее построения обязательно должна быть проверена на согласованность суждений ЛПР.

Основные требования, которые предъявляются к согласованности суждений ЛПР, состоят в выполнении им условий согласованности и транзитивности, рассмотренных ранее (см. этап 2)

Для обнаружения несогласованности суждений ЛПР, при построении им матрицы парных сравнений, Саати предложил проводить оценку степени согласованности (или отношения согласованности – ОС), которое вычисляется по следующему выражению:

$$OC = \frac{IC}{R} = \frac{(\lambda_{\max} - m_m)}{(m_m - 1) \cdot R} \qquad (5.13)$$

при этом $IC = \frac{(\lambda_{\max} - m_m)}{(m_m - 1)}$ (5.14)

где: IC - значение индекса согласованности для реальной матрицы парных сравнений факторов

R - значение индекса согласованности для несимметрических матриц, заполненных случайным образом. Это значение зависит от порядка матрицы парных сравнений факторов и приведено в табл. 5.9

m_m – размерность матрицы парных сравнений факторов; следует иметь в виду, что она также соответствует максимальному собственному значению согласованной идеальной матрицы парных сравнений;

$m_m = n$ - для матрицы парных сравнений критериев

$m_m = m$ - для матрицы парных сравнений вариантов

$\lambda_{\max}$ - максимальное собственное значение реальной матрицы парных сравнений факторов

Для матрицы парного сравнения факторов имеем следующее:

- если $OC \le 0{,}1$ то суждения ЛПР согласованы и матрица является согласованной;
- если $OC > 0{,}1$ то суждения ЛПР не согласованы, поэтому следует заново провести парное сравнение факторов рассматриваемой матрицы

Для вычисления $\lambda_{\max}$, используемого в выражении (5.13), Саати предложил следующий алгоритм:

1) В матрице парных сравнений факторов суммируются элементы каждого столбца;

2) Сумма элементов каждого столбца этой матрицы умножается на соответствующие нормализованные компоненты вектора весов факторов, определенного из этой же матрицы, и получаем числа λ_j, количество которых соответствует количеству факторов этой таблицы;

3) Полученные числа λ_j суммируем и значение этой суммы обозначаем как $\lambda_{\max}$

Таблица 5.9

Значение индекса согласованности (R) для несимметрических матриц в зависимости от порядка матрицы парных сравнений факторов.

m	3	4	5	6	7	8	9	10	11	12	13
R	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,54	1,56

Пример 5.3 При реорганизации организационной структуры АСОИиУ **п**еред руководителем фирмы стоит задача выбрать помещение для размещения службы ремонта и обслуживания компьютерной техники. Все необходимые данные ему предоставили сотрудники аналитического отдела.

Решение. На первом этапе руководитель фирмы (ЛПР) выполняет структуризацию процесса принятия решения и разрабатывает иерархическую трехуровневую схему факторов: цель, критерии выбора помещения, варианты сравниваемых помещений с полным набором их характеристик..

Цель ЛПР - выбрать недорогое для содержания и удобное с точки зрения территориального расположения помещение для размещения службы ремонта и обслуживания компьютерной техники. Для достижения поставленной цели используются критерии:

К1 – возможность расширения помещения за счет рядом расположенных помещений с целью развития службы компьютерной поддержки;

К2 – территориально удобное расположение помещения;

К3 – стоимость ремонта и содержания помещения.

На основании данных, предоставленных сотрудниками аналитического отдела, ЛПР выделяет четыре варианта помещений, которым дает соответствующее кодовое наименование В1, В2,В3 и В4, для выбора среди них наиболее приемлемого.

На втором этапе ЛПР выполняет парное сравнение трех критериев, а также парное сравнение четырех вариантов помещений по каждому из критериев, используя упрощенную вербальную шкалу, приведенную в табл 5.7.

Составленная ЛПР матрица парных сравнений критериев приведена в табл. 5.10. , а матрицы парных сравнений вариантов помещений по каждому из критериев приведены соответственно в табл. 5.11, 5.12 и 5.13..

На третьем этапе ЛПР сначала вычисляет собственные вектора каждого из рассматриваемых факторов: для критериев использует выражение (5.7), а для вариантов помещений - выражение (5.8) , а затем вычисляет коэффициенты важности этих факторов, используя соответственно выражения (5.9) и (5.10). Полученные данные ЛПР заносит в соответствующие таблицы парного сравнения этих факторов: для критериев в

табл 5.10, а для вариантов помещений, с учетом критерия, по которому проводилось их сравнение, соответственно в табл. 5.11 - 5.13.

Таблица 5.10

Матрица сравнения критериев

Критерий	К1	К2	К3	Собственный вектор	Вес критерия
К1	1	3	5	2,47	0,650
К2	1/3	1	3	0,848	0,230
К3	1/5	1/3	1	0,48	0,120

Таблица 5.11

Матрица сравнения вариантов по критерию К1

Вариант	В1	В2	В3	В4	Собственный вектор	Вес критерия
В1	1	1	0,333	0,2	0,508	0,106
В2	1	1	0,333	0,333	0,577	0,120
В3	3	3	1	1	1,732	0,362
В4	5	3	1	1	1,968	0,412

Таблица 5.12

Матрица сравнения вариантов по критерию К2

Вариант	В1	В2	В3	В4	Собственный вектор	Вес критерия
В1	1	0,11	0,2	014	0,23	0,050
В2	9	1	3	1	2,28	0,430
В3	5	0,33	1	1	1,14	0,220
В4	7	1	1	1	1,63	0,300

Таблица 5.13

Матрица сравнения вариантов по критерию К3

Вариант	В1	В2	В3	В4	Собственный вектор	Вес критерия
В1	1	3	5	9	3,4	0,560
В2	0,33	1	3	7	1,63	0,270
В3	0,2	0,33	1	5	0,76	0,130
В4	0,11	0,14	0,2	1	0,23	0,040

На четвертом этапе ЛПР, используя выражение (5.11), определяет показатель качества каждого варианта решения (в данном случае – это варианты помещения В1, В2, В3 и В4) , а затем согласно выражения (5.12) определяет наилучший вариант решения, те. выбирает наиболее приемлемое, с его точки зрения, помещение для размещения службы.

Результаты этих расчетов таковы:

$$Y_1 = 0,65 \cdot 0,106 + 0,23 \cdot 0,05 + 0,12 \cdot 0,56 = 0,1517$$

$$Y_2 = 0,65 \cdot 0,120 + 0,23 \cdot 0,43 + 0,12 \cdot 0,27 = 0,2077$$

$$Y_3 = 0,65 \cdot 0,362 + 0,23 \cdot 0,22 + 0,12 \cdot 0,13 = 0,2906$$

$$Y_4 = 0,65 \cdot 0,412 + 0,23 \cdot 0,30 + 0,12 \cdot 0,04 = 0,3390$$

$$Y_4 = \max_j Y_j = 0,3390$$

Анализ приведенных результатов показывает, что наилучшим решением является выбор помещения, обозначенного как В4.

На пятом этапе ЛПР осуществляет проверку согласованности своих суждений, учитывающую проверку корректности и безошибочности своих действий при заполнении матриц парного сравнения, Эту проверку ЛПР выполняет в следующей последовательности:

1) вычисляет максимальное собственное значение каждой из четырех матриц парных сравнений факторов по ранее приведенному алгоритму (смотри этап.5) В результате расчетов имеем

$\lambda_{\max K} = 3{,}117$ - максимальное собственное значение матрицы парных сравнений критериев;

максимальные собственные значения матриц парных сравнений вариантов помещений по критериям К1, К2 и К3 соответственно имеют значения $\lambda_{\max 1} = 4{,}023$, $\lambda_{\max 2} = 4{,}233$, $\lambda_{\max 3} = 4{,}2015$

2) определяет из табл 5.9 значение индекса согласованности для несимметрических матриц, заполненных случайным образом, и получает для них следующие значения

$R_K = 0{,}58 \qquad R_1 = R_2 = R_3 = 0{,}90$

3) вычисляет отношение согласованности для каждой матрицы парных сравнений используя выражение (5.13).

На основании проведенных расчетов получены следующие результаты:

$OC_K = 0{,}1 \quad OC_1 = 0{,}0074 \quad OC_2 = 0{,}085 \quad OC_3 = 0{,}082$

Для каждой из матриц выполняется условие согласованности $OC \le 0{,}1$, поэтому суждения ЛПР следует считать согласованными и выбор варианта помещения В4 в качестве наилучшего вполне обоснованным.

5.4 Выбор организационно-управленческих решений при модернизации АСОИиУ на основе упрощенного метода анализа иерархий

При данном методе осуществляется только парное сравнение критериев и не проводится парное сравнение альтернативных вариантов по каждому критерию. Вместо парного сравнения альтернативных вариантов по каждому из локальных критериев, проводится ранжирование вариантов по указанным критериям, используя при этом полную или базовую вербально-цифровую шкалу качества (табл 5.14 и 5.15) и все полученные данные заносятся только в одну таблицу (матрицу) сравнения вариантов по критериям

Градации этих шкал расположены так, что наивысшая вербальная оценка (например, “отлично”) получает наивысший балл (например, 5), а наихудшая оценка соответственно наименьший балл

Таблица 5.14

Полная вербально-цифровая шкала качества

Оценка качества	Балл	Оценка качества	Балл
отлично	5,0	плохо	2,0
очень хорошо	4,5	очень плохо	1,5
хорошо	4,0	сверх плохо	1,0
выше среднего	3,5	неудовлетворительно	0,5
удовлетворительно	3,0	неприемлемо	0,0
ниже среднего	2,5	-	-

Таблица 5.15

Базовая вербально-цифровая шкала качества

Оценка качества	Балл	Оценка качества	Балл
отлично	5,0	плохо	2,0
хорошо	4,0	сверх плохо	1,0
удовлетворительно	3,0	неприемлемо	0,0

Применение метода на практике состоит из нескольких этапов.

Этап 1. Структуризация процесса принятия решения. Задачи, решаемые на этом этапе, аналогичны задачам, решаемым на этапе 1 в разделе 5.3

Этап 2. Последовательное парное сравнение критериев. Все критерии упорядочивают по степени их важности. Парное сравнение критериев проводится аналогично этапу 2 раздела 5.3

Этап 3. Вычисление коэффициентов важности критериев сравниваемых вариантов и рангов вариантов, соответствующих этим критериям. Весовые коэффициенты критериев (α_i) вычисляются аналогично этапу 3 раздела 5.3 по выражению (5.9)..

Далее проводится последовательное ранжирование альтернативных вариантов по каждому из локальных критериев в соответствии с одной из выбранных для этих целей вербально-цифровой шкалой, приведенной в табл 5.14 или 5.15. Составляется матрица

сравнения альтернативных вариантов по локальным критериям - $\left\| r_{ij} \right\|$ Количество строк этой матрицы соответствует количеству локальных критериев, а количество столбцов - количеству альтернативных вариантов, подлежащих сравнению. Поэтому r_{ij} - это элемент матрицы, который численно равен количеству баллов, которое дают j -му альтернативному варианту по i -му локальному критерию.

Этап 4. Определение наилучшего варианта решения Выбор наилучшего варианта решения осуществляется в следующей последовательности:

- вычисляют показатель качества , т.е интегральный критерий, Y_j каждого j-го варианта решения ($j = 1,...m$,), используя следующее выражение

$$Y_j = \sum_{i=1}^{n} \alpha_i \cdot r_{ij} \qquad \text{где} \quad j = 1,....m \qquad (5.15)$$

- выбирают вариант решения (l) , для которого показатель качества Y_l принимает максимальное значение, и считают этот вариант решения наилучшим.

$$Y_l = \max_j Y_j \qquad \text{где} \quad j = 1,....m \qquad (5.16)$$

Этап 5. Проверка согласованности суждений ЛПР. Степень корректности заполнения матрицы парных сравнений критериев и согласованности суждений оценивают на основании отношения согласованности (ОС), которое вычисляется по выражению (5.13)

Выполнение этого этапа аналогично выполнению этапа 5 раздела 5.3.

Пример 5.4 Организация решила провести модернизацию АСОИиУ. Менеджеры организации провели детальный анализ целого ряда компьютерных фирм, которые оказывают подобные услуги, и на его основе выделили пять фирм, которые в полной мере отвечают всем предъявляемым требованиям. Из этих пяти фирм необходимо выбрать одну, которая в наибольшей степени удовлетворяет требованиям данной организации.

Решение. На первом этапе выполняют структуризацию процесса принятия решения и получают иерархическую трехуровневую схему факторов: цель, критерии, компьютерные фирмы, а также выбирают эти факторы

Цель организации - выбрать компьютерную фирму, которая за приемлемое время, недорого и качественно выполнит модернизацию АСОИиУ и обеспечит последующее надежное ее функционирование.

Для достижения поставленной цели используют следующие критерии:

К1 - стоимость модернизации АСОИиУ и последующего обслуживания (тыс.руб);

К2 – время от разработки технического задания до момента ввода АСОИиУ в опытную эксплуатацию (количество дней);

К3 – качество установки, определяемое на основе анализа работы действующих сетей;

К4 – срок действия фирмы на рынке коммерческих услуг;

К5 – финансовое положение компьютерной фирмы;

К6 - территориальное размещение фирмы и возможность оперативной связи;

К7 - готовность фирмы оперативно и качественно выполнять заказы по обслуживанию АСОИиУ, которые не указаны в договоре, заключенном между фирмой и организацией.

Всем пяти выделенным фирмам ЛПР дает соответствующее кодовое наименование (варианты В1, В2 , В3, В4 и В5) для выбора среди них наиболее приемлемого.

На втором этапе выполняют парное сравнение семи критериев используя фундаментальную вербально-числовую шкалу (см. табл 5.8). Матрица парных сравнений критериев приведена в табл. 5.16

Таблица 5.16

Матрица парных сравнений критериев
выбора фирмы поставщика компьютерных услуг

Критерии	К1	К2	К3	К4	К5	К6	К7
К1	1	2	4	5	6	8	9
К2	1/2	1	3	4	5	6	7
К3	1/4	1/3	1	2	3	5	6
К4	1/5	1/4	1/2	1	3	5	6
К5	1/6	1/5	1/3	1/3	1	2	3
К6	1/8	1/6	1/6	1/5	1/2	1	2
К7	1/9	1/7	1/6	1/6	1/3	1/2	1

На третьем этапе вычисляют коэффициенты важности критериев, используя последовательно выражения (5.7) и (5.9). Расчеты позволили получить следующие результаты:

$$\alpha_1 = 0,425 \qquad \alpha_2 = 0,250 \qquad \alpha_3 = 0,116 \qquad \alpha_4 = 0,085$$

$$\alpha_5 = 0,057 \qquad \alpha_6 = 0,037 \qquad \alpha_7 = 0,030$$

Далее проводят последовательное ранжирование альтернативных вариантов по каждому из локальных критериев в соответствии с базовой вербально-цифровой шкалой качества, (см. табл 5.15) По этим данным составляютт матрицу сравнения альтернативных вариантов по локальным критериям, приведенную в табл 5.17

В эту же таблицу записывают весовые коэффициенты критериев.

Таблица 5.17

Матрица сравнения альтернативных вариантов по локальным критериям

Локальный критерий	Оценки альтернативных вариантов по критериям					α_i
	B1	B2	B3	B4	B5	
K1	3	4	4	3	5 (*)	0,425
K2	5 (*)	4	3	5 (*)	3	0,250
K3	2	5 (*)	3	2	5 (*)	0,116
K4	5 (*)	4	2	5 (*)	3	0,085
K5	4	2	3	5 (*)	2	0,057
K6	5 (*)	2	4	2	3	0,037
K7	4	3	4	5 (*)	5 (*)	0,030
$Y_j = \sum_{i=1}^{n} \alpha_i \cdot r_{ij}$	3,715	3,900	3,660	3,690	4,085	
$Y_k^* = \max_j Y_j$					4,08	

Примечание. Знаком (*) - отмечены лучшие варианты решения по рассматриваемому локальному критерию

На четвертом этапе, используя выражение (5.15), вычисляют интегральные критерии для каждого варианта решения и записывает их в дополнительную строку в табл 5.17. Затем, согласно выражению (5.16), выбирают в качестве наилучшего варианта решения - вариант B5, для которого интегральный критерий принимает наибольшее значение.

На пятом этапе осуществляют проверку согласованности суждений, относительно заполнении матрицы парного сравнения критериев. Проверку выполняют в следующем порядке:

1) вычисляют максимальное собственное значение матрицы парных сравнений критериев по алгоритму (см. этап.5 раздела 5.3)

В результате расчетов имеем $\lambda_{\max} = 7,46$

2) определяют из табл 5.9 значение индекса согласованности для несимметрических матриц размерности семь, заполненных случайным образом, и получают значение $R = 1,32$

3) вычисляют отношение коэффициента согласованности для матрицы парных сравнений критериев используя выражение (5.13). На основании проведенных расчетов получены следующие результаты:

$$OC = \frac{IC}{R} = \frac{(\lambda_{\max} - n)}{(n-1) \cdot R} = \frac{(7,46-7)}{6 \cdot 1,32} = 0,058$$

Так как для матрицы парных сравнений критериев выполняется условие $OC \le 0{,}1$, то суждения, относительно ранжирования критериев, следует считать согласованными, и выбор варианта В5 в качестве наилучшего варианта вполне обоснованным

Ранжирование вариантов по упрощенному методу аналитической иерархии дало следующие результаты: $B5 \succ B2 \succ B1 \succ B4 \succ B3$. При этом значение глобального критерия наилучшего варианта отличается от значения глобального критерия наихудшего варианта менее чем на 10%, что показывает достаточную близость всех альтернативных вариантов друг другу по интегральному критерию.

Контрольные вопросы и задания к главе 5.

1. Поясните различия процессов принятия решения в условиях определенности и в условиях полной неопределенности.
2.. Поясните различие между критерием Лапласа и критерием Вальда.
3. Поясните различие между критерием Лапласа и критерием Ходжа-Лемана.
4. Поясните различие между критерием Вальда и критерием Ходжа-Лемана..
5.. Какие критерии следует отнести к разряду оптимистических.
6. Какие критерии следует отнести к разряду пессимистических
7. Поясните достоинство метода сбалансированного критерия.
8. Поясните основные правила построения “дерева целей”.
9. Поясните основные этапы процесса принятия решения методом Паттерн.
10. Поясните различие метода анализа иерархий и метода “дерево целей”.
11. Перечислите отличия метода аналитической иерархии от упрощенного метода аналитической иерархии.
12. Поясните отличие метода аналитической иерархии от метода взвешенной суммы локальных критериев.
13.. Напишите основные этапы процесса принятия решений при использования метода аналитической иерархии.
14. Напишите выражение для оценки степени согласованности суждений ЛПР при построении матрицы парного сравнения критериев.
15. Напишите основные этапы процесса принятия решений при использовании упрощенного метода аналитической иерархии.

Литература к главе 5

Основная

Мадера А.Г. Моделирование и принятие решений в менеджменте. Руководство для будущих топ-менеджеров / А.Г. Мадера. М.: ЛКИ, 2010.
688 с.

Постников В.М. Методы принятия решений в системах организационного управления: учеб. пособие./ В.М. Постников, В.М. Черненький. М.: Изд-во МГТУ им. Н.Э. Баумана. 2014. 205 с.

Дополнительная

Колемаев В.А. Математические методы и модели исследования операций. М.: ЮНИТИ-ДАНА. 2009. 592 с.

Мендель А.В. Модели принятия решений. / А.В. Мендель. М.: ЮНИТИ-ДАНА. 2010
463 с.

Глава 6 Выбор вариантов развития АСОИиУ на основе экспертных методов

6.1 Выбор организационно-управленческих решений при модернизации АСОИиУ с использованием метода Дельфи

Метод экспертных оценок Дельфи обычно используют при выборе вариантов решений, касающихся совершенствования и развития АСОИиУ. Основу метода составляют следующие принципы сбора и обработки экспертной информации:

1) эксперты должны дать четкий ответ на каждый вопрос анкеты;

2) опрос экспертов может проводиться как в один, так и в несколько туров, в ходе проведения которых они постоянно уточняют свои ответы за счет ознакомления обмена мнениями с другими экспертами;

3) итоговый результат заключается в получении количественной оценки специалистов по каждому из рассматриваемых альтернативных вариантов с целью выбора преобладающего мнения для определения лицом принимающим решение (ЛПР) наилучшего варианта решения.

Использование метода Дельфи на практике предусматривает последовательное выполнение следующих этапов:

Этап 1. Разработка цели, задач и исходных данных для проведения экспертного анализа ЛПР задает исходные данные и формирует цель проведения экспертного опроса, которая должна позволять получать количественную оценку для каждого варианта решения.

Этап 2 Формирование рабочей группы экспертов для проведения экспертного анализ. ЛПР формирует рабочую группу экспертов. Для определения числа экспертов z можно использовать следующую формулу:

$$z > 0,5(\frac{0,3}{b} + 5) \qquad (6.1)$$

где b- ошибка результата экспертного анализа (0< b<1);

Этап 3 Разработка анкеты для проведения опроса экспертов. Анкета, разработанная ЛПР, должна:

1) включать корректные и понятные вопросы;

2) использовать язык среды анкетирования;

3) иметь вид шаблона, в котором каждый эксперт может дать только один вариант оценки из предложенного ему набора оценок. При этом набор оценок, или возможных ответов n, в анкете, обычно определяют по формуле

$$n = \log_2 z + 1 \qquad (6.2)$$

Этап 4. Организация и проведение опроса экспертов рабочей группы. При проведении опроса экспертов ЛПР должен учитывать следующее:

- опрос экспертов может проводиться как в один, так и в несколько туров, в ходе проведения которых ответы экспертов ими же уточняются;
- эксперты могут знакомиться с результатами предыдущего тура опроса;
- эксперты обязательно обосновывают выставленные оценки, если эти оценки существенно отличаются от оценок большинства экспертов;
- при проведении опроса сохраняется анонимность экспертов по отношению друг к другу, что исключает влияние научного авторитета или должностного положения отдельных экспертов;
- после проведения каждого тура эксперты имеют возможность уточнить свои оценки за счет учета дополнительных факторов;
- в случае нескольких туров время между двумя последовательными турами должно быть достаточным для того, чтобы эксперты могли при необходимости детально ознакомиться с материалами своих коллег.

Следует иметь в виду, что уже после трех туров разброс мнений экспертов уменьшается, а общее мнение группы экспертов, выраженное в виде их индивидуальных оценок, стабилизируется.

Этап 5. Обработка результатов опроса экспертов и формирование итогового решения. На данном этапе ЛПР проводит обработку результатов опроса экспертов и формирует итоговое решение, которое заключается в выявлении преобладающего мнения и получении количественной оценки специалистов по рассматриваемому вопросу .

В процессе обработки оценок экспертов используются понятия медианы и моды.

Медиана- численное значение признака, которым обладает центральный член экспертного ряда, при условии, что ряд составлен в порядке возрастания значений рассматриваемого признака.

На практике порядковый номер N члена ранжированного ряда, на который приходится медиана, определяется следующим образом::

- если ряд с четным числом экспертов z , то $N = z/2$

- если ряд с нечетным числом экспертов z, то $N = (z+1)/2$

Медиана Me вычисляется по следующей интерполяционной формуле

$$Me = X_{k-1} + \frac{N - F_{k-1}}{f_k} \cdot h_k \qquad (6.3)$$

Где X_{k-1} - нижняя граница интервала, в котором находится медиана

N - порядковый номер члена ряда, на который приходится медиана

F_{k-1} - накопленная частота ответов экспертов во всех интервалах, предшествующих тому, в котором находится медиана

f_k - частота ответа экспертов интервала, в котором находится медиана

h_k - длина интервала рассматриваемого признака

Мода – значение рассматриваемого признака, которое наиболее часто встречается в ранжированном ряду. Мода Mo вычисляется по следующей интерполяционной формуле

$$Mo = X_{k-1} + \frac{(f_k - f_{k-1})}{(f_k - f_{k-1}) + (f_k - f_{k+1})} \cdot h_k \qquad (6.4)$$

X_{k-1} - нижняя граница интервала, в котором находится мода

f_k - частота ответов экспертов, соответствующих модовому интервалу

f_{k-1} - частотаответов экспертов, предшествующих модовому интервалу

f_{k+1} - частота ответов экспертов, соответствующих интервалу, следующему за модовым

h_k - длина интервала рассматриваемого признака

На основt результатов обработки ответов экспертов ЛПР принимает решение, которое соответствует медиане или моде, а также может найти компромисс между ними.

При всех очевидных достоинствах метод Дельфи имеет и ряд недостатков, к основным из которых относят:

- трудность проведения экспертного опроса с большим количеством экспертов, да к тому же еще в течение нескольких туров;
- необходимость очень четкого, корректного и краткого изложения в анкетах всей требуемой для экспертов информации;
- необходимость тщательного анализа ответов всех экспертов, особенно в случаях, когда мнения некоторых из них существенно отличаются от мнения большинства членов рабочей группы.

Пример 6.1. Фирма имеет большое количество филиалов, разбросанных по региону. В главном офисе и каждом филиале круглосуточно функционируют АСОИиУ на базе ЛВС. В целях увеличения эффективности функционирования АСОИиУ руководство фирмы решило издать руководящий материал по рациональной организации их эксплуатации. Один из пунктов этого руководящего материала касается выбора режима фрагментации данных на жестком диске сервера. Для разрешения возникшей проблемной ситуации руководитель фирмы (ЛПР) предложил использовать метод Дельфи.

Решение. На первом этапе ЛПР формирует цель проведения экспертного опроса: необходимо определить средний интервал времени между двумя последовательными фрагментациями жесткого диска сервера для увеличения производительности работы системы.

На втором этапе ЛПР из состава сотрудников филиалов формирует рабочую группу экспертов в количестве 123 человек

На третьем этапе ЛПР разрабатывает анкету для проведения опроса экспертов, основной вопрос которой приведен в первом столбце табл. 11.1. Число допустимых ответов на приведенный в табл 11.1 вопрос установлено по формуле 11.2

На четвертом этапе ЛПР организует и проводит опрос экспертов, а полученные данные заносит в табл 6.1, во второй столбец. После этого ЛПР формирует в табл. 6.1 третий столбец.

Таблица 6.1

Результаты опроса экспертов относительно рассматриваемой проблемной ситуации

Время между двумя последовательными фрагментациями диска (дни) (*)	Количество ответивших экспертов (частота ответов экспертов)	Накопленная частота ответов экспертов
12 - 24	5	5
24 – 36	10	15
36 - 48	10	25
48 - 60	15	40
60 - 72	15	55
72 - 84	30	85
84 - 96	20	105
96 - 108	10	115
108 – 120	8	123

(*) - указаны рабочие дни, подразделения фирмы работают ежедневно, кроме воскресных и праздничных дней, 80 - среднее число рабочих дней в квартал.

На пятом этапе ЛПР обрабатывает результаты опроса экспертов. Используя выражения (6.3) и (6.4) ЛПР получает соответственно численные значения медианы (M) и моды (MD) для времени фрагментации жесткого диска сервера, которые приведены ниже.

$$N = (m+1)/2 = 124/2 = 62$$

$$Me = 72 + \frac{(62-55)}{30} \cdot 12 = 74,8 \quad \text{дня}$$

$$Mo = 72 + \frac{(30-15)}{(30-15)+(30-20)} \cdot 12 = 79,2 \quad \text{дня}$$

Таким образом, рекомендуемое экспертами время между двумя последовательными фрагментациями данных на жестком диске сервера составляет

медиана $Me = 74,8$ дня , мода $Mo = 79,2$ дня

На основе полученных данных ЛПР принимает важное и практически удобное решение: выполнять фрагментацию данных на жестком диске сервера один раз в квартал

6.2 Выбор организационно-управленческих решений при модернизации АСОИиУ с использованием метода экспертных оценок.

Основу метода экспертных оценок составляет ранжирование альтернативных вариантов по степени их важности группой экспертов, а также анализ степени согласованности мнений экспертов по выбранному уровню предпочтительности рассматриваемых вариантов. Метод также используют и для ранжирования параметров сравниваемых вариантов с целью их деления на группы важности, при этом параметры, подлежащие ранжированию, обычно называют факторами.

Применение метода экспертных оценок на практике предполагает последовательное выполнение следующих этапов.

Этап 1. Формирование цели проведения экспертного анализа Цель проведения экспертного анализа состоит в следующем:

- провести ранжирование исходных альтернативных вариантов модернизации АСОИиУ для выбора среди них наилучшего;
- выполнить ранжирование факторов, влияющих на выбор оборудования и отобрать среди них существенные.

Этап 2. Формирование исходного набора рассматриваемых вариантов или рассматриваемых факторов. Исходный набор альтернативных вариантов (или факторов) обычно формируется в результате анализа исследуемого процесса и представляется в виде строк таблицы, в которой названию каждого варианта ставится в соответствие определенный код (например, первому варианту–код В1, а второму–код В2 и т.д, Факторам аналогично присваиваются коды –Х1, Х2 и т.д.). Столбцы этой таблицы соответствуют оценкам, которые дает эксперт вариантам.. Число вариантов или факторов, подлежащих анализу и ранжированию, рекомендуется брать не более 10. Увеличение их числа ведет к сложности ранжирования в условиях необходимости обеспечения согласованной оценки экспертов

Этап 3. Формирование состава экспертной группы и оценка уровня компетентности экспертов и группы в целом. Число экспертов z в группе должно быть не меньше числа вариантов сравнения m, т. е. $(z \geq m)$;

Уровень компетентности экспертов оценивается следующим образом

$$K_{эj} = \frac{K_{aj} + K_{uj}}{K_{am} + K_{um}} = \frac{K_{aj} + K_{uj}}{2} \qquad (6.5)$$

где $K_{эj}$ - коэффициент, отражающий уровень компетентности j – го эксперта; K_{aj} - коэффициент, отражающий уровень аргументации j – го эксперта; K_{uj} -коэффициент, отражающий уровень информированности j – го эксперта

Коэффициенты $K_{эj}$, K_{aj}, K_{uj} могут принимать значения от 0 до 1.

K_{am} *и* K_{um} - максимальные оценки коэффициентов K_{aj}, K_{uj}, равны 1.

Коэффициент представительности или компетентности экспертной группы вычисляется по следующей формуле:

$$Q = \frac{1}{z} \cdot \sum_{j=1}^{z} K_{эj} \qquad (6.6)$$

$$0,67 \leq Q \leq 1 \qquad (6.7)$$

Если условие (6.10) выполняется, то экспертная группа считается компетентной, иначе состав экспертной группы формируется заново.

Этап 4. Формирование окончательного набора рассматриваемых альтернативных вариантов и состава экспертной группы. ЛПР формирует набор вариантов (или факторов), подлежащих ранжированию, и окончательный состав компетентной рабочей группы экспертов

Этап 5. Проведение экспертного опроса. Каждый эксперт заполняет анкету и ранжирует все альтернативные варианты по степени их важности. При этом наиболее значимому варианту эксперт присваивает значение ранга равное 1, соответственно второму по значимости варианту значение ранга равное 2, и т. д., Наименее значимому варианту эксперт присваивает ранг равный m.

Каждый эксперт работает в стандартизованной ранговой системе. Если эксперт не в состоянии указать порядок мест важности двух или более вариантов, поскольку, по его мнению, они все важны в одинаковой степени, этим вариантам он присваивает один и тот же ранг. Такие экспертные варианты принято называть связанными.

Численное значение ранга связанных вариантов представляет собой среднее значение суммы мест этих вариантов в ранговой системе эксперта.

Результаты ранжирования предложенных экспертам вариантов, сводятся в единую таблицу, например, как показано в табл.6.2 (столбцы 1-7).

Таблица 6.2

Результаты ранжирования вариантов экспертами рабочей группы

Код варианта	Ранг, присвоенный варианту экспертом						r_i	$(r_i - r)$	$(r_i - r)^2$
	Э1	Э2	Э3	Э4	Э5	Э6			
1	2	3	4	5	6	7	8	9	10
В1	5	5	5	4	4	5	28	10	100
В2	1	1	2	2	1	3	10	- 8	64
В3	4	4	4	5	5	4	26	8	64
В4	2	2,5	1	1	2,5	1	10	- 8	64
В5	3	2,5	3	3	2,5	2	16	- 2	4
r_j	15	15	15	15	15	15			$\sum_{i=1}^{n} (r_i - r)^2 = 296$

Этап 6. Обработка результатов экспертного опроса После проведения опроса экспертов и заполнения таблицы вида табл. 6.2 проводится математическая обработка результатов экспертного опроса. При этом используются следующие обозначения:
z – число экспертов в рабочей группе;
m - число вариантов, подлежащих ранжированию экспертами;

r_{ij} - ранг, присвоенный j - ым экспертом i – му варианту (i = 1, m) , (j = 1, z)

$\alpha_{эj}$ - уровень компетентности j - го эксперта

Далее последовательно вычисляем следующие показатели:

r_i - суммарный средний ранг i –го варианта, присвоенный ему экспертами

$$r_i = z \cdot \sum_{j1}^{z} \alpha_{эj} \cdot r_{ij} \qquad (6.8)$$

Если уровень компетентности экспертов одинаков, то $\alpha_{эj} = 1/z$ и

$$r_i = \sum_{j=1}^{m} r_{ij} \qquad (6.9)$$

$\hat{r_j}$ - сумму рангов, присвоенных j - ым экспертом всем вариантам, которые подлежат ранжированию

$$\hat{r_j} = \sum_{i=1}^{m} r_{ij} = \frac{m(m+1)}{2} \qquad (6.10)$$

r - суммарный средний ранг всех вариантов, определяемый условиями проведения опроса экспертов.

$$r = \frac{1}{m} \sum_{i=1}^{m} \sum_{j=1}^{z} r_{ij} = \frac{(m+1)z}{2} \qquad (6.11)$$

S - сумму квадратов отклонений суммарных средних рангов каждого из вариантов от суммарного среднего ранга вариантов

$$S = \sum_{i=1}^{n} (r_i - r)^2 \qquad (6.12)$$

$S_{\max}$ - максимально возможную сумму квадратов отклонений суммарных средних рангов каждого из вариантов от суммарного среднего ранга вариантов с учетом наличия связанных вариантов.

$$S_{\max} = \frac{1}{12} z^2 (m^3 - m) - z \sum_{j=1}^{z} T_j \qquad (6.13)$$

где $$T_j = \frac{1}{12} \cdot \sum_{k=1}^{Hj} (t_{jk}^3 - t_{jk}) \qquad (6.14)$$

T_j -коэффициент, учитывающий наличие связанных вариантов у j -го эксперта; Hj - число групп одинаковых рангов вариантов у j -го эксперта;

k - номер группы одинаковых рангов вариантов у j -го эксперта (k = 1, Hj);

t_{jk} - число одинаковых рангов вариантов в k -ой группе у j - го эксперта.

Если связанных вариантов у экспертов нет, то

$$S_{\max} = \frac{1}{12} z^2 (m^3 - m) \qquad (6.15)$$

W - Коэффициент конкордации, т.е. коэффициент согласованности мнений экспертов, определяется по формуле Кендалла

$$W = \frac{S}{S_{\max}} = \frac{S}{\frac{1}{12} z^2 (m^3 - m) - z \sum_{j=1}^{z} T_j} \qquad (6.16)$$

Если связанных факторов у экспертов нет, то

$$W = \frac{12 \cdot S}{z^2 (m^3 - m)} \qquad (6.17)$$

При значении $W \geq 0,7$ считается, что мнения экспертов согласованы

оценку значимости коэффициента конкордации, по критерию χ^2. При этом величина $Wz(m-1)$ имеет χ^2 распределение с $\upsilon = m-1$ степенями свободы. Если имеются связанные факторы у экспертов, то расчетное значение χ^2 распределения с $\upsilon = m-1$ степенями свободы рассчитывается по следующей формуле:

$$\chi^2 = \frac{S}{\frac{1}{12} z \cdot n(m+1) - \frac{1}{m-1} \sum_{j=1}^{z} T_j} \qquad (6.18)$$

Если связанные варианты у экспертов отсутствуют, то формула упрощается и принимает следующий вид

$$\chi^2 = \frac{12 \cdot S}{z \cdot m(m+1)} \qquad (6.19)$$

Табличное значение критерия χ^2_T определяется при уровне значимости $\alpha = 0,05$ и указанном ранее числе степеней свободы (см. табл. 6.7) . Если $\chi^2 > \chi^2_T$, т.е. расчетное значение больше табличного, то с вероятностью 95% можно утверждать, что мнения экспертов являются вполне согласованными.

Если $\chi^2 < \chi^2_T$, то согласованность у экспертов отсутствует

ранжирование вариантов по уровню их важности выполняется согласно процедуре Борда, чем меньше ранг, тем вариант более значим, при этом вариант B_l , у которого наименьший ранг - наилучший вариант.

$$r_l = \min_i r_i \qquad (6.20)$$

Этап 7. Анализ результатов работы экспертной группы. После проведения опроса экспертов и обработки результатов этого опроса обычно делается анализ работы экспертной группы, в котором указываются:

- уровень компетентности экспертов и рабочей группы экспертов в целом;
- степень согласованности мнений экспертов;
- ранжированный ряд вариантов или уровни важности факторов;

Качественную оценку степени согласованности мнений экспертов, при известном численном значении коэффициента конкордации дают:

- по шкале, предложенной Марголиным, и приведенной в табл. 6.3
- по шкале Харрингтона, приведенной в табл. 6.4

Таблица 6.3

Оценка степени согласованности мнений экспертов по шкале, предложенной Марголиным

№	Числовое значение коэффициента конкордации	Оценка степени согласованности мнений экспертов
1	$0 \le W \le 0,1$	отсутствует
2	$0,1 < W \le 0,3$	очень слабая
3	$0,3 < W \le 0,5$	слабая
4	$0,5 < W \le 0,7$	умеренная
5	$0,7 < W \le 0,9$	высокая
6	$0,9 < W \le 1,0$	очень высокая

аблица 6.4

Оценка степени согласованности мнений экспертов по шкале Харрингтона

№	Числовое эначение коэффициента конкордации	Оценка степени согласованности мнений экспертов
1	$0 \le W \le 0,2$	очень низкая
2	$0,2 < W \le 0,37$	низкая
3	$0,37 < W \le 0,64$	средняя
4	$0,64 < W \le 0,8$	высокая
5	$0,8 < W \le 1,0$	очень высокая

Пример 6.2 ЛПР сформировал группу из шести квалифицированных экспертов ($z = 6$), предоставил им подробные материалы по пяти исходным альтернативным вариантам развития АСОИиУ ($m = 5$) и поставил перед ними задачу: выбрать наилучший вариант развития АСОИиУ и провести ранжирование вариантов по степени их важности.

Решение. Результаты ранжирования исходных альтернативных вариантов развития АСОИиУ, которые выполнили эксперты с использованием стандартизованной ранговой системы, приведены в табл 6.3, (столбцы 2-7), где по мнению экспертов ранг 1 соответствует самому лучшему варианту, а ранг 5 – наихудшему.

Результаты расчетов, полученные ЛПР на основе использования выражений (6.9 – 6.12) приведены в табл. 6.2, (столбцы 8 -10), а $S = 296$.

Расчеты, проведенные ЛПР по выражениям (6.13) и (6.14), показали, что $S_{\max} = 354$, при этом

$$T_1 = T_3 = T_4 = T_6 = 0 \qquad T_2 = \frac{1}{12} \cdot \left[(2^3 - 2) \right] = 0,5 \qquad T_5 = \frac{1}{12} \cdot \left[(2^3 - 2) \right] = 0,5$$

Значение коэффициента конкордации, вычисленное по выражению (6.16), равно $W = 0,836$. Оценка значимости коэффициента конкордации, по критерию χ^2, проведенная по выражению (6.18), показала, что расчетное значение $\chi^2 = 20,06$.

Табличное значение критерия χ_T^2 при уровне значимости $\alpha = 0,05$ и числе степеней свободы $\upsilon = n - 1 = 4$, согласно табл. 6.7, $\chi_T^2 = 9,488$

Поскольку $\chi^2 > \chi_T^2$, т.е. расчетное значение больше табличного, то с вероятностью 95% можно утверждать, что мнения экспертов являются вполне согласованными.

При этом, согласно данным, приведенным в табл 6.3 и 6.4, учитывающим численное значение коэффициента конкордации, степень согласованности мнений экспертов соответственно высокая и очень высокая.

Ранжирование вариантов по степени их предпочтительности ЛПР осуществляет на основании численного значения суммарного среднего ранга варианта, присвоенного ему экспертами, и определяемого по выражению (6.9). Поэтому имеем: $r_1 = 28$

$r_2 = 10 \qquad r_3 = 26 \qquad r_4 = 10 \qquad r_5 = 16$

Наилучшими вариантами развития АСОИиУ согласно (6.20) являются два варианта В2 и В4, имеющие наименьший и равный ранг, а ранжирование вариантов по степени их предпочтительности имеет вид:

.

$$\text{B2} \approx \text{B4} \succ \text{B5} \succ \text{B3} \succ \text{B1}$$

Пример 6.3 ЛПР сформировал группу из шести квалифицированных экспертов, обеспечил их необходимой информацией, которая приведена в табл 6.5, и поставил перед ними задачу проранжировать указанные пять факторов и выделить среди них основные, на которые следует обратить особое внимание при выборе поставщика оборудования АСОИиУ.

Таблица 6.5

Факторы, влияющие на выбор поставщика оборудования АСОИиУ

№ п/п	Код фактора	Наименование фактора
1	X1	Известность фирмы - производителя оборудования и весомость ее марки.
2	X2	Соответствие паспортных характеристик приобретаемого оборудования реальным возможностям этого оборудования
3	X3	Уровень сервисного обслуживания, который может предложить компания поставщик оборудования
4	X4	Показатель надежность/цена приобретаемого оборудования
5	X5	Уровень организации продаж оборудования, который имеет компания поставщик оборудования

Решение. Результаты ранжирования факторов, полученные экспертами с использованием стандартизованной ранговой системы, приведены в табл 6.6, (столбцы 2-7), где ранг 1 соответствует самому важному фактору,

Таблица 6.6

Результаты ранжирования вариантов экспертами рабочей группы

Код фактора	Ранг, присвоенный фактору экспертом						r_i	$(r_i - r)$	$(r_i - r)^2$
	Э1	Э2	Э3	Э4	Э5	Э6			
1	2	3	4	5	6	7	8	9	10
X1	1	1	2	2	1	1	8	-10	100
X2	2	2	1	1	3	3	12	- 6	36
X3	4	3	4	3	2	2	18	0	0
X4	3	5	3	5	4	4	24	6	36
X5	5	4	5	4	5	5	28	10	100
r_j	15	15	15	15	15	15			$\sum_{i=1}^{n} (r_i - r)^2 = 272$

Результаты расчетов, полученные ЛПР на основе использования выражений (6.9 – 6.12) приведены в табл. 6.6 (столбцы 8 -10), при этом $S = 272$.

Расчеты, проведенные ЛПР по выражениям (6.15), показали, что $S_{\max} = 360$.

Значение коэффициента конкордации, вычисленное по выражению (6.17) равно $W = 0,755$. Оценка значимости коэффициента конкордации, по критерию χ^2, проведенная по выражению (6.19), показала, что расчетное значение $\chi^2 = 18,12$.

Табличное значение критерия χ_T^2 при уровне значимости $\alpha = 0,05$ и числе степеней свободы $\upsilon = n - 1 = 4$, согласно табл. 6.7 равно $\chi_T^2 = 9,5$

Поскольку $\chi^2 > \chi^2_T$, т.е. расчетное значение больше табличного, то с вероятностью 95% можно утверждать, что мнения экспертов являются вполне согласованными. При этом, согласно данных, приведенных в табл 6.3 и 6.4, учитывающих численное значение коэффициента конкордации, степень согласованности мнений экспертов высокая.

Ранжирование факторов по степени их предпочтительности ЛПР осуществляет на основании численного значения суммарного среднего ранга фактора, присвоенного ему экспертами, и определяемого по выражению (6.9). Поэтому имеем: $r_1 = 8$ $r_2 = 12$ $r_3 = 18$ $r_4 = 24$ $r_5 = 28$

Согласно выражению (6.20) наиболее важным является фактор под кодом X1, имеющий наименьший ранг, а ранжирование факторов по степени их важности имеет следующий вид:. $X1 \succ X2 \succ X3 \succ X4 \succ X5$

Таблица 6.7

Распределение хи-квадрат Вероятность $P\{\chi 2 >= \chi 2(\alpha ; \upsilon)\}$

α - уровень значимости, υ – число степеней свободы

Число степеней свободы υ	Уровень значимости α		
	0,10	0,05	0,01
1	2,706	3,841	6,635
2	4,605	5,991	9,210
3	6,251	7,815	11,341
4	7,779	9,488	13,277
5	9,236	11,070	15,086
6	10,645	12,592	16,812
7	12,017	14,067	18,475
8	13,362	15,507	20,090
9	14,684	16,919	21,665
10	15,986	18,307	23,209
11	17,275	19,675	24,725
12	18,549	21,026	26,217
13	19,812	22,362	27,688
14	21,064	23,685	29,141
15	22,307	24,995	30,578

Контрольные вопросы и задания к главе 6

1. Перечислите основные принципы, составляющие основу метода Дельфи.
2. Поясните назначение основных этапов практического применения метода Дельфи.
3. Дайте практические рекомендации по использованию метода Дельфи.
4.. Поясните назначение основных этапов практического использования метода экспертного анализа.
5.. Приведите выражения для выбора количественного и качественного состава экспертной группы.
6.. Приведите выражение для количественной оценки степени согласованности мнений экспертной группы.
7. Приведите примеры вербально-числовых шкал для качественной оценки степени согласованности мнений экспертной группы.
8. Дайте практические рекомендации по использованию метода экспертного анализа.
9. Поясните условия применения метода экспертного анализа.
10. Поясните как можно определить весовые коэффициенты факторов при использовании метода экспертного анализа.

Литература к главе 6

Основная

Постников В.М. Методы принятия решений в системах организационного управления: учеб. пособие./ В.М. Постников, В.М. Черненький. М.: Изд-во МГТУ им. Н.Э. Баумана. 2014. 205 с.

Дополнительная

Амелин С.В. Экономико-математические методы и модели в дипломном проектировании и выпускных квалификационных работах. Часть 1./ С.В. Амелин. Воронеж: ВГТУ, 2011. 188 с.

Орлов А.И. Организационно-экономическое моделирование. Теория принятия решений./А.И. Орлов. М.: КНОРУС. 2011. 568 с.

Глава 7. Выбор варианта развития АСОИиУ на основе методов теории массового обслуживания.

7.1. Основные понятия теории массового обслуживания

Эффективность функционирования АСОИиУ во многом определяют ее аппаратно-программная и организационная структуры. Работа АСОИиУ обычно связана с обслуживанием запросов, поступающих от клиентов в случайные моменты времени. При этом обслуживание этих запросов часто имеет случайный характер. Все это создает неравномерность в работе ресурсов обслуживающей системы, в качестве которых могут быть как аппаратно-программные средства, так и персонал, занятый их обслуживанием. что порождает либо простой и недогрузки, либо перегрузки ресурсов системы. Перегрузка ресурсов означает наличие очередей в обслуживающей системе и увеличение времени обслуживания запросов клиентов.

В связи с этим необходима сравнительная оценка различных вариантов модернизации аппаратно-программной и организационной структуры существующей АСОИиУ, и анализ перспективных вариантов ее развития для обеспечения эффективности функционирования системы и ее компонент с целью выявления перегруженных ресурсов, поиска резервов и выработки в конечном итоге рекомендаций, направленных на дальнейшее увеличение эффективности работы АСОИиУ.

Для определения основных временных и загрузочных характеристик функционирования АСОИиУ и их основных компонент, на этапах проектирования, модернизации/реорганизации довольно часто используют аналитическое моделирование. Основу аналитического моделирования систем составляет аналитическая модель, полученная при определенных допущениях и предположениях, которая позволяет достаточно просто и быстро получить такие основные характеристики функционирования обслуживающих систем, как среднее время реакции системы на запрос пользователя, загрузка системы, среднее число заявок в очереди и в системе и т.д.

При разработке аналитических моделей систем, как правило, используют методы теории массового обслуживания (методы ТМО), учитывающие вероятностный характер информационных процессов протекающих в этих системах

Предметом изучения ТМО являются системы массового обслуживания (СМО) и стохастические сети массового обслуживания (СеМО).

СМО - это система обслуживания потока заявок, поступающих на ее вход при заданном законе и порядке обслуживания этих заявок с учетом параметров структуры самой обслуживающей системы..

СеМО- это совокупность взаимосвязанных СМО. Структуру СеМО можно представить в виде графа, вершины которого соответствуют отдельным СМО, а дуги вероятностям переходов заявок между этими СМО.

Модели СМО и СеМО удобны, как для анализа сложных систем и организационных структур, так и для анализа отдельных подсистем, входящих в их состав.

В составе каждой СМО можно выделить следующие компоненты:

1. Источники заявок, определяющие входящие в СМО потоки заявок. Количество источников заявок определяет количество входящих в СМО потоков заявок (n). В зависимости от характера источника заявок различают источники с бесконечным числом заявок и источники с конечным числом заявок. В первом случае источник генерирует неограниченное число заявок в соответствии с заданной функцией распределения интервала времени между поступающими заявками и его работа не зависит от обслуживающей системы. Во втором случае в системе циркулирует конечное, и обычно постоянное, число заявок.

СМО с бесконечным числом заявок называются разомкнутыми, а с конечным числом заявок - замкнутыми.

2. Входящий поток заявок - это совокупность всех типов заявок, поступающих на вход СМО. Обычно его задают функцией распределения интервалов времени между моментами поступления двух соседних заявок для каждого потока, т. е. средним значением интервала времени между заявками, и коэффициентом вариации этого времени.

Одной из важнейших характеристик входящего потока является его интенсивность, равная среднему числу заявок поступающих в единицу времени. Величина обратная интенсивности определяет средний интервал времени между двумя последовательными заявками.

Наиболее часто в качестве входящего потока при анализе СМО используют простейший поток, который обладает следующими свойствами:

- стационарность, когда вероятность поступления заявок в систему в интервале [t, t+h] зависит лишь от величины h ;
- ординарность, когда на бесконечно малом промежутке времени h поступает не более одной заявки;

- отсутствие последействия, когда вероятность поступления заявок в систему в интервале [t, t+h] не зависит от количества заявок поступивших в систему до момента времени t.

Для простейшего потока интервалы времени между двумя последовательными заявками – это непрерывные случайные величины с экспоненциальной функцией распределения $F(\tau)=1-e^{-\lambda\tau}$ и плотностью распределения $f(\tau)=\lambda e^{-\lambda\tau}$. где λ- интенсивность поступления потока заявок в систему в единицу времени.

3. Механизм обслуживания заявок, который включает:

- длительность обслуживания заявок (среднее время и коэффициент вариации времени обслуживания заявок). На практике наиболее часто используют экспоненциальное распределение длительности обслуживания заявок в обслуживающем аппарате (ОА), которое описывается функцией распределения времени обслуживания F(τ) и плотностью распределения f (τ):

$$F(\tau)=1-e^{-\mu\tau} \qquad \text{и} \qquad f(\tau)=\mu e^{-\mu\tau}$$

где μ - интенсивность обслуживания заявок в СМО в единицу времени.

Среднее время обслуживания заявки $M(\tau)$ и дисперсию времени обслуживания заявки $D(\tau)$ определяют из следующих формул:

$$M(\tau)=1/\mu \qquad \text{и} \qquad D(\tau)=1/\mu^2$$

- количество обслуживающих аппаратов (ОА) в обслуживающей системе, равное (с), которые могут одновременно обслуживать поступающие заявки. По количеству ОА в обслуживающей системе различают: одноканальные СМО, если в системе один ОА и многоканальные СМО, если в системе несколько ОА.

- пропускная способность обслуживающей системы - $\mu_{сис}$, которая зависит от числа обслуживающих аппаратов (с) и средней интенсивности обслуживания заявок (μ_i) каждым ОА.

$$\mu_{сис}=\sum_{i=1}^{c}\mu_i$$

Обычно считают, что СМО, включают только однотипные ОА

- количество мест в очереди на обслуживание (m), т. е. число заявок, которое может находиться в очереди и ожидать начала обслуживания, если все ОА заняты обслуживанием. Число мест заявок в очереди на обслуживание определяет доступность обслуживания. В зависимости от числа мест в очереди различают СМО с отказами и СМО без отказов.

В СМО с отказами число мест в очереди на обслуживание конечно и вследствие вероятностного характера, как входящего потока заявок, так и процесса их обслуживания, существует вероятность того, что поступившая на вход СМО заявка застанет все ОА и все места в очереди занятыми, т.е. получит отказ в обслуживании.

В СМО без отказов заявка либо сразу поступает на обслуживание, если имеется хотя бы один свободный ОА, либо поступает в очередь бесконечной длины и там находится до начала обслуживания.

- дисциплина формирования очереди. По правилу формирования очереди различают СМО с общей очередью и СМО с несколькими очередями. При общей очереди заявки заполняют очередь в порядке поступления. В случае наличия нескольких очередей, как правило, очереди неоднородны по значимости. Более важные заявки поступают в более приоритетные для обслуживания очереди;

- дисциплина обслуживания очереди определяет правила выбора заявок из очереди на обслуживание. Имеют место бесприоритетные и приоритетные дисциплины обслуживания.

В общем случае возможны различные комбинации дисциплин формирования и обслуживания очереди, что порождает достаточно широкий спектр вариантов управления процессами обработки заявок в СМО.

7.2 Показатели и критерии оценки эффективности функционирования СМО.

Показатели оценки эффективности функционирования СМО - это количественные показатели, характеризующие уровень выполнения СМО возложенных на нее функций по обслуживанию заявок при определенном наборе рабочих параметров СМО. К основным показателям оценки качества обслуживания заявок в СМО, обычно относят следующие показатели:

Вероятность обслуживания заявок ($P_{обс}$) - это вероятность того, что произвольно выбранная из входящего потока с интенсивностью λ заявка будет обслужена, т.е. окажется в выходящем потоке обслуженных заявок с интенсивностью $\lambda_{вых}$.Обычно эту вероятность обслуживания заявок называют также относительной пропускной способностью СМО, обозначают символом (q) и определяют из следующего выражения:.

$$P_{обс} = q = \lambda_{вых} / \lambda$$

Вероятность потери заявок ($P_{отк}$) - это вероятность того, что произвольно выбранная из входящего потока с интенсивностью λ заявка окажется в потоке заявок с интенсивностью $\lambda_{отк}$, .которым будет отказано в обслуживании. $P_{отк} = 1 - P_{обс}$

Среднее время ожидания заявки в очереди (W). В общем случае время ожидания – это случайная величина, равная сумме длительностей интервалов времени, в течение которых заявка находится в очереди, начиная с момента поступления заявки на вход СМО и кончая моментом, когда заявка последний раз покидает очередь уходя из очереди на обслуживание.

Среднее время ожидания является суммой двух составляющих: среднего времени ожидания начала обслуживания и среднего времени ожидания в прерванном состоянии, когда обслуживается более приоритетная заявка.. Первая составляющая равна промежутку времени между моментом поступления заявки на вход СМО и моментом первого назначения заявки на обслуживание. Вторая составляющая равна сумме промежутков времени между моментами поступления заявки, обслуживание которой было прервано, снова в очередь, и моментами поступление этой заявки на дообслуживание.

Среднее время пребывания заявки в СМО (T).- это время равно среднему промежутку времени от момента поступления заявки на вход СМО до момента появления ее в выходящем потоке. Среднее время пребывания заявки в СМО равно сумме среднего времени нахождения заявки в очереди и среднего времени обслуживания в ОА.

$$T = W + 1/\mu$$

Средняя длина очереди (Q) - это среднее число заявок, находящихся в очереди. Для систем без потерь средняя длина очереди связана со средним временем ожидания, согласно формулы Литтла, следующим соотношением:

$$Q = W \cdot \lambda$$

Среднее число заявок в СМО (L) - это среднее суммарное число заявок, которое находится в очереди и в обслуживающих аппаратах. Для систем без потерь среднее число заявок в системе связано со средним временем пребывания, согласно формулы Литтла, следующим соотношением:

$$L = T \cdot \lambda$$

Загрузка обслуживающего аппарата СМО (ρ) - это коэффициент использования ОА, вычисляют по следующей формуле

$$\rho = \lambda /(\mu \cdot c)$$

Загрузка обслуживающей системы (φ) - это среднее число занятых обслуживающих аппаратов. Если обслуживающие аппараты однородны, то φ определяется из следующего выражения

$$\varphi = c \cdot \rho$$

В качестве критерия эффективности функционирования СМО обычно выбирают один, наиболее важный показатель, или несколько показателей, при этом критерий являются некоторой функцией свертки набора этих показателей.. Критерий эффективности функционирования СМО является средством оценки соответствия СМО возложенным на нее функциям. В качестве простейшего и широко используемого на практике критерия, как правило, используют критерий, который минимизирует общую стоимость обработки заявок в СМО. Его можно представить в следующем виде:

E_l - стоимость обработки заявок в СМО, имеющей вариант структурной организации l, который является наилучшим с точки зрения выбранного критерия эффективности .

E_j - стоимость обработки заявок в СМО имеющей вариант структурной организации j

В - количество возможных вариантов построения СМО

При этом стоимость обработки заявок в СМО, имеющей j-ый вариант структурной организации, определяется из следующего выражения:

$$E_l = \min_j E_j = \min_j \left[\; c \cdot \rho \cdot \sum_{i=1}^{n} e_{1ij} \cdot (1/\mu_{ij}) + \sum_{i=1}^{n} e_{2ij} \cdot T_{ij} \; \right] \qquad j = 1,2,,\mathrm{B} \qquad (7.1)$$

Где E_l - стоимость обработки заявок в СМО, имеющей вариант структурной организации l, который является наилучшим с точки зрения выбранного критерия эффективности .

E_j - стоимость обработки заявок в СМО имеющей вариант структурной организации j

В - количество возможных вариантов построения СМО

e_{1ij} - стоимость единицы времени обслуживания заявки i - го типа в СМО, имеющей вариант структурной организации j;

e_{2ij} - стоимость единицы времени пребывания заявки i - го типа: в СМО, имеющей вариант структурной организации j;

$1/\mu_{ij}$ - среднее время обслуживания заявки i - го типа в СМО, имеющей вариант структурной организации j;

T_{ij} - среднее время пребывания заявки i - го типа в СМО., имеющей вариант структурной организации j;

ρ - загрузка ОА

c - число ОА

n - число типов заявок, поступающих на вход СМО.

7.3 Аналитическая модель оценки работы канала связи

Для формализованного описания работы канала связи АСОИиУ с помехами используют разомкнутую СМО, имеющую символическое обозначение М/М/1 с обратной связью. В этой СМО после обработки заявки в обслуживающем аппарате, заявка с вероятностью «р», повторно поступает на обработку в СМО., что учитывает повторную передачу данных из-за возможных сбоев в работе канала связи, которые имеют вероятностный характер.

Рассматриваемую СМО отличают следующие особенности:

- учитывает экспоненциальное распределение времени передачи данных через канал связи;

- учитывает влияние окружающей среды, т. е. помех, на повторную передачу данных за счет наличия обратной связи;

- позволяет исследовать работу канала связи и оценить его реальные характеристики.

В состав показателей оценки качества функционирования рассматриваемой СМО обычно входят:

- загрузка ОА СМО, имитирующая загрузку работы канала связи;
- среднее число заявок в очереди СМО, соответствующих числу запросов на передачу данных, находящихся в очереди канала;
- среднее число заявок в СМО, соответствующее среднему суммарному числу запросов в очереди и в канале связи;
- среднее время нахождения заявок в очереди СМО, соответствующее среднему времени нахождения запросов в очереди на передачу через канал связи;
- среднее время пребывания заявок в СМО, соответствующее среднему суммарному времени пребывания запроса в очереди и в канале связи;
- вероятность $P(t)$, с которой заявка будет обслужена, соответствующая вероятности, с которой запрос на передачу данных через канал связи будет выполнен за требуемое время.

Для оценки показателей качества функционирования СМО введем следующие обозначения:

λ - интенсивность входящего в СМО потока заявок;

t_O - среднее время обработки заявок в ОА СМО;

$\mu_O = 1/t_O$ - интенсивность обработки заявок в ОА СМО;

ρ - загрузка ОА СМО;

Q - среднее число заявок в очереди СМО;

L - среднее число заявок в системе (в очереди и на обслуживании);

W - среднее время нахождения заявки в очереди;

T - среднее время пребывания заявки в системе;

$P(t_{прб} < t)$ -вероятность, с которой время пребывания заявки в системе должно быть менее заданной величины. ($t_{прб}$).

Для оценки характеристик функционирования рассматриваемой СМО, отображающей работу канала связи АСОИиУ с помехами, следует использовать аналитические выражения в указанном порядке:

1. Определяем интенсивность $\lambda_{вх}$ реального входящего потока заявок в СМО с учетом возможной повторной обработки заявок с вероятностью p. Уравнение потоков для СМО имеет вид $\lambda + \lambda_{вх} \cdot p = \lambda_{вх}$ (7.2)

Решая уравнение (12.2), получаем

$$\lambda_{вх} = \frac{\lambda}{1-p} = \lambda\alpha \qquad (7.3)$$

Где $\alpha = \frac{1}{1-p}$ число входов заявки в ОА за время пребывания ее в СМО.

2. Определяем загрузку обслуживающего аппарата СМО

$$\rho = \frac{\lambda_{вх}}{\mu} \qquad (7.4)$$

3. Определяем среднее число заявок в очереди

$$Q = \frac{\rho^2}{1-\rho} \qquad (7.5)$$

4. Определяем среднее число заявок в СМО

$$L = Q + \rho = \frac{\rho}{1-\rho} \qquad (7.6)$$

5. Определяем, используя формулу Литтла, среднее время ожидания заявок в очереди с учетом того, что заявка «α» раз поступает на обслуживание за время пребывания ее в СМО

$$W = \frac{Q \cdot \alpha}{\lambda_{вх}} \qquad (7.7)$$

6. Определяем, используя формулу Литтла, среднее время пребывания заявок в СМО с учетом того, что заявка «α» раз поступает на обслуживание за время пребывания ее в СМО

$$T = \frac{L \cdot \alpha}{\lambda_{вх}} \qquad (7.8)$$

7. Определяем вероятность, с которой заявка будет пребывать в СМО не более времени $t_{прб}$

$$P(t_{прб} < t) = 1 - e^{-t/T} \qquad (7.9)$$

Для быстрой сравнительной оценки альтернативных вариантов каналов связи, только по показателю среднее время доставки пакетов данных, следует использовать следующее выражение:

$$T = \frac{L \cdot \alpha}{\lambda_{вх}} = \frac{\rho}{(1-\rho)\cdot(1-p)\cdot\lambda_{вх}} = \frac{1}{(1-p)\mu - \lambda} \qquad (7.10)$$

Пример 7.1 Входящий поток заявок в канал связи составляет 4 запроса/с, Интенсивность, с которой канал может передавать данные составляет 10 запросов/с. Возможны три варианта организации работы канала связи в зависимости от варианта прокладки кабельной системы.. В первом варианте прокладки кабельной системы помехи очень маленькие, практически отсутствуют и ими можно пренебречь Во втором варианте они составляют 20%., а в третьем – 50%.

Следует оценить влияние помех на характеристики функционирования канала связи.

Исходные данные. $\lambda = 4$ заявки/с, $\mu = 10$ заявок/с $\rho = \lambda / \mu = 0,4$

Для вариантов 1, 2 и 3 соответственно имеем: $p = 0,0$ $p = 0,2$ $p = 0,5$

Решение. Последовательно используя формулы 12.3-12.8, для оценки работы канала без помех и с помехами, получаем результаты, которые приведены в табл. 7.1

Таблица 7.1

Сравнение результатов работы канала связи в трех режимах

Показатель сравнения	Варианты сравнения каналов связи		
	Канал без помех	Канал с помехами $p = 0,2$	Канал с помехами $p = 0,5$
p	0	0,2	0,5
α	1	1,25	2
$\lambda_{вх}$ заявок/с	4	5	8
ρ	0,4	0,5	0,8
Q заявок	0,267	0,5	3,2
L заявок	0,667	1,0	4,0
W с	0,067	0,125	0,8
T с	0,167	0,250	1,0

Среднее время пребывания запроса в канале связи, из-за наличия помех, существенно увеличивается. Так, если загрузка канала связи составляет 40% ($\rho = 0,4$), то имеем:

- наличие помех с уровнем 20% приводит к увеличению времени передачи запроса через канал связи, по сравнению с каналом без помех, в 1,5 раза;
- увеличение уровня помех в 2,5 раза (с 20% до 50%,) приводит к увеличению времени передачи запроса через канал связи в 4 раза.

Пример 7.2 Сравнить три альтернативных варианта организации работы каналов связи, исходные данные которых приведены в табл.7.2,, и выбрать среди них наилучший вариант по показателю минимальное время передачи запроса данных через канал. В канал поступают запросы с интенсивностью $\lambda = 20$ запросов/с

Решение После подстановки исходных данных в формулу (7.10) получаем результаты, приведенные в табл. 7.2

Таблица 7.2

Исходные данные и результаты сравнения альтернативных вариантов организации работы каналов связи

Показатель сравнения	Варианты сравнения		
	В1	В2	В3
Исходные данные			
μ запросов/с	30	25	22
p	0,3	0,1	0,05
Результаты сравнения			
$\mu(1-p)$ запросов/с	21	22,5	20,9
T с	0,5	0,4 (*)	1,11

Примечание. Знаком (*) отмечен наилучший вариант

На основании сравнения результатов работы каналов связи, приведенных в табл.12.2 , получаем, что наилучшим вариантом работы канала связи является вариант В2.

7.4. Аналитическая модель оцени работы службы ремонта и обслуживания компьютеров.

Для описания работы службы ремонта и обслуживания компьютеров следует использовать замкнутую СМО, имеющую символическое обозначение M / M / C / N / ПППО / N.

Эту СМО, отличают следующие особенности:

- учитывает экспоненциальное распределение времени наработки на отказ у каждого компьютера, экспоненциальное распределение времени ремонта компьютера каждым специалистом - ремонтником,
- имеет «С» идентичных обслуживающих аппаратов, отражающих работу «С» специалистов – ремонтников одного уровня квалификации;
- имеет общую очередь заявок, соответствующую очереди компьютеров на ремонт, с дисциплиной выбора заявок из очереди на обслуживание «первый пришел–первым обслужен» (ПППО);
- имеет «N» источников заявок, поступающих на обслуживание в ОА, которые соответствуют количеству компьютеров в системе.
- источник заявок в любой момент времени может находиться в одном из двух состояний: активном, отражает работу исправного компьютера, и пассивном, отражает работу компьютера, который отказал. При переходе из активного состояния в пассивное состояние источник заявок посылает в обслуживающую систему заявку, соответствующую заказу на ремонт компьютера. Заявка сразу поступает на обслуживание, если имеется свободный ОА, или в очередь, если все ОА заняты. Из очереди заявка поступает на обслуживание в соответствии с дисциплиной обслуживания ПППО.

Показатели оценки качества функционирования рассматриваемой СМО - это количественные показатели, характеризующие уровень выполнения СМО возложенных на нее функций. В состав этих показателей входят:

- загрузка ОА (генератора заявок), имитирующего работу компьютера (ρ_e);
- загрузка ОА, имитирующего работу ремонтника (ρ_o);
- среднее количество заявок в очереди СМО (компьютеров в очереди на ремонт), (Q);
- среднее суммарное количество заявок в очереди СМО и в ОА (суммарное количество компьютеров в очереди на ремонт и ремонтируемых), (L);
- среднее время нахождения заявок в очереди СМО (компьютеров в очереди на ремонт), (W);

- среднее время пребывания заявок в СМО, т.е.суммарное среднее время пребывания заявок в очереди и в ОА (среднее время пребывания компьютера в неисправном состоянии) (T).
- среднее количество источников заявок, находящихся в активном состоянии, т.е. среднее количество исправно работающих компьютеров ($n = N - L$), где N- общее количество источников заявок в СМО, равное количеству компьютеров в системе.

Введем следующие обозначения:

$t_{НО}$ - среднее время наработки на отказ одного компьютера;

$t_О$ - среднее время ремонта одного компьютера;

$\mu_{НО} = 1/t_{НО}$ - интенсивность отказов одного компьютера

$\mu_О = 1/t_О$ - интенсивность ремонта компьютера

N - количество компьютеров

C - количество специалистов, занятых ремонтом компьютеров

P_k -вероятность, что (k) компьютеров находятся в состоянии отказа.

$\Psi = \mu_{НО} / \mu_О$ - коэффициент отношения интенсивности наработки на отказ к интенсивности восстановления работоспособности компьютера

Для оценки характеристик функционирования рассматриваемой замкнутой СМО M/M/C/N/ПППО/N следует использовать аналитические выражения, которые известны в ТМО как аналитическая модель ремонтника.

Порядок расчета замкнутой СМО вида M/M/C/N/ППО/N.

1. Определяем вероятности состояний рассматриваемой замкнутой СМО используя выражения (7.11 – 7.13)

$$P_0 = \left[\sum_{k=0}^{c} \frac{N! \cdot \Psi^k}{k! \cdot (N-k)!} + \sum_{k=c+1}^{N} \frac{N! \cdot \Psi^k}{c^{k-c} \cdot c! \cdot (N-k)!} \right]^{-1} \qquad (7.11)$$

$$P_k = \frac{N! \cdot \Psi^k}{k! \cdot (N-k)!} P_0 \qquad 1 \le k \le c \qquad (7,12)$$

$$P_k = \frac{N! \cdot \Psi^k}{c^{k-c} c! \cdot (N-k)!} P_0 \qquad 1 \le k \le c \qquad (7,13)$$

2. Определяем Q - среднее количество компьютеров, находящихся в очереди на ремонт

$$Q = \sum_{k=c}^{N} (k-c) \cdot P_k \qquad (7,14)$$

3. Определяем L - среднее количество компьютеров, находящихся в неисправном состоянии, т.е в очереди на ремонт и на ремонте

$$L = \sum_{k=1}^{N} k \cdot P_k \qquad (7,15)$$

4. Определяем U - среднее количество компьютеров, которое непосредственно ремонтируются специалистами.

$$U = L - Q \qquad (7,16)$$

5. Определяем ρ_O - коэффициент загрузки одного специалиста, занятого ремонтом компьютеров $\rho_O = U / C$ (7,17)

6. Определяем T_p - среднее время пребывания компьютера в неисправном состоянии (в очереди на ремонт и ремонте)

$$T_p = T_ц - t_{но} \qquad (7,18)$$

Где $T_ц$ - среднее время цикла для компьютера (время наработки на отказ плюс время нахождения в неисправном состоянии)

Согласно правилу Литтла имеем

$$N = \lambda \cdot T_ц = \lambda \cdot (T_p + t_{но}) \qquad (7,19)$$

$$L = \lambda \cdot T_p \qquad (7,20)$$

Где λ - интенсивность потока заявок, циркулирующих в СМО, равная интенсивности потока отказов компьютеров в системе

Приравниваем выражения (7.19) и (7.20) и находим T_p

Имеем $$T_p = \frac{L \cdot t_{но}}{N - L} \quad (7{,}21)$$

7. Определяем W - среднее время нахождения компьютера в очереди на ремонт $$W = T_p - t_o \quad (7{,}22)$$

8. Определяем $T_ц$ - среднее время цикла для компьютера

$$T_ц = T_p + t_{но} \quad (7{,}23)$$

9. Определяем ρ_e - коэффициент загрузки компьютера, т.е. долю времени, в течение которого он находится в исправном состоянии

$$\rho_e = \frac{t_{но}}{T_ц} \quad (7{,}24)$$

10. Определяем n - среднее количество исправных компьютеров

$$n = (N - L) \quad (7{,}25)$$

11. Определяем режим работы службы ремонта и обслуживания компьютеров. Согласно организационно-технологическому процессу, протекающему в системе, справедливы следующие выражения

$$\rho_e = \frac{\lambda \cdot t_{но}}{N} \quad (7{,}26)$$

$$\rho_o = \frac{\lambda \cdot t_0}{C} \quad (7{,}27)$$

Приравнивая выражения (П4.16) и (П4.17) получаем

$$\frac{\rho_e}{\rho_o} = \frac{C \cdot t_{но}}{N \cdot t_o} \quad (7{,}28)$$

Анализируя выражение (П4.18) получаем:

- если $$\frac{\rho_e}{\rho_o} = \frac{C \cdot t_{но}}{N \cdot t_o} = 1 \quad (7{,}29)$$

то система сбалансированная, компьютеры и специалисты, занятые их ремонтом имеют один и тот же коэффициент загрузки;

-

если $$\frac{\rho_e}{\rho_o} = \frac{C \cdot t_{но}}{N \cdot t_o} >> 1 \quad (7{,}30)$$

то компьютеры загружены намного больше, чем специалисты, занятые их ремонтом, и, следовательно, в системе мало неисправных компьютеров;

- если $\frac{\rho_e}{\rho_o} = \frac{C \cdot t_{но}}{N \cdot t_o} << 1$ (7,31)

то компьютеры загружены намного меньше, чем специалисты, занятые их ремонтом, и, следовательно, в системе много неисправных компьютеров.

Пример 7.2 В организации имеется 100 компьютеров. Время наработки компьютера на отказ подчиняется экспоненциальному закону, со средним значением 800 часов, время ремонта и восстановления компьютера, выполняемое одним специалистом также починяется экспоненциальному закону со средним значением 8 часов

Специалист, занятый ремонтом компьютеров, получает за один час рабочего времени зарплату 200 рублей. Простой одного компьютера в течение одного часа приводит к тому, что организация теряет 350 рублей. Компьютеры, как и специалист, занятый их ремонтом работают каждый месяц 25 рабочих дней по 8 часов в день, т. е. 200 часов в месяц.

Необходимо определить, сколько специалистов для ремонта компьютеров нужно организации, чтобы минимизировать общие финансовые потери, включающие убытки от неисправных компьютеров и заработанную плату, выплачиваемую специалистам, занятым ремонтом этих компьютеров.

Исходные данные: $N = 100$ компьютеров $t_{но} = 800$ час $t_o = 8$ час

Заработанная плата специалиста за один час составляет $S_1 = 200$ руб/час

Финансовые потери организации от неисправного компьютера за один час составляют $S = 350$ руб/(компьютер час)

Решение. Результаты расчетов, проведенные по формулам (7,11- 7,25), приведены в табл.7.3

Таблица 7.3

Характеристики функционирования СМО M/M/C/N/ПППО/N

Параметр	Вариант 1	Вариант 2	Вариант 3
Количество ремонтников	$c=1$	$c=2$	$c=3$
P_0	0,07570	0,33760	0,36584
Q	6,64575	0,30084	0,04110
L	7,57005	1,28796	1,03078
$U=L-Q$	0,92430	0,98712	0,98969
$\rho_o=U/C$	0,92430	0,49356	0,32990
$n=N-L$	92,43000	98,71200	98,96920
$\rho_e=n/N$	0,92430	0,98712	0,98969
W	57,52000	2,43690	0,33211
T_p	65,52000	10,43690	8,33200
$T_ц=T_p+t_{но}$	865,52000	810,43690	808,33200
ρ_e/ρ_o	1	2	3

Убытки организации (Y_i) при i- м варианте организации работы службы ремонта компьютеров определяются по формуле

$$\mathrm{Y_i}=m_i\cdot S_i+L_i\cdot S \qquad (7,32)$$

Где m_i – количество специалистов занятых ремонтов компьютеров при i- ом варианте организации работы службы ремонта компьютеров.

При этом наилучший вариант (d) организации работы службы ремонта компьютеров определяется по формуле

$$\mathrm{Y_d}=\min_i \mathrm{Y_i} \qquad (7,33)$$

После подстановки в выражение (6,32) исходных данных и результатов расчетов, приведенных в табл. 6.3, получаем:

для варианта 1 $\mathrm{Y_1}=S_1+L_1\cdot S=200+7,57\cdot 350=2843,50$ руб/час

для варианта 2 $\mathrm{Y_2}=2\cdot S_1+L_2\cdot S=2\cdot 200+1,288\cdot 350=850,80$ руб/час

для варианта 3 $\mathrm{Y_3}=3\cdot S_1+L_3\cdot S=3\cdot 200+1,031\cdot 350=960,85$ руб/час

Анализ полученных результатов позволяет утверждать, что согласно выражению (7,33) наилучшим вариантом решения является вариант 2 Поэтому фирме следует организовать работу службу ремонта компьютеров на базе двух сотрудников.

Далее в табл. 7.4 – 7.6 приведены характеристики функционирования СМО M/M/C/N/ПППО/N при различных значениях параметров $t_{но}$, t_o, N и C для проведения самостоятельного анализа и оценки эффективности работы службы ремонта и обслуживания компьютеров.

Таблица 7.4

Характеристики функционирования СМО M/M/C/N/ППО/N при $N=100$ компьютеров, $t_{НО}=600$ час, $t_О=8$ час

Параметр	Вариант 1	Вариант 2	Вариант 3
Количество ремонтников	$c=1$	$c=2$	$c=3$
P_0	0,000923	0,208730	0,257518
Q	24,07000	0,878762	0,12731
L	25,0692	2,1830	1,4414
$U=L-Q$	0, 9991	1,3042	1,3141
$\rho_О=U/C$	0,9991	0,6500	0,4380
$n=N-L$	74,9308	97,8170	98,5586
$\rho_{РС}=n/N$	0,74931	0,97817	0,98558
$T_р$	200,739	13,390	8,775
$T_ц=T_р+t_{НО}$	800,739	613,390	608,775
$\rho_{РС}/\rho_О$	0,75	1,50	2,25

Таблица 7.5

Характеристики функционирования СМО M/M/C/N/ППО/N при $N=100$ компьютеров, $t_{НО}=600$ час, $t_О=6$ час

Параметр	Вариант 1	Вариант 2	Вариант 3
Количество ремонтников	$c=1$	$c=2$	$c=3$
P_0	0,0757	0,3376	0,36584
Q	6,64575	0,30084	0,0411
L	7,57005	1,28796	1,03078
$U=L-Q$	0,9243	0,9871	0,9896
$\rho_О=U/C$	0,9243	0,49356	0,329897
$n=N-L$	92,43	98,712	98,9692
$\rho_{РС}=n/N$	0,9243	0,98712	0,989692
W	43,14	1,8286	0,249
$T_р$	49,14	7,8286	6,24908
$T_ц=T_р+t_{НО}$	649,14	607,8286	606,2498
$\rho_{РС}/\rho_О$	1	2	3

Таблица 7.6

Характеристики функционирования СМО M/M/C/N/ППО/N
при $N = 100$ компьютеров, $t_{HO} = 400$ час, $t_O = 6$ час

Параметр	Вариант 1	Вариант 2	Вариант 3
Количество ремонтников	$c = 1$	$c = 2$	$c = 3$
P_0	0,00005	0,157253	0,2144
Q	32,3353	1,4406	0,2046
L	33,3353	2,8971	1,6794
$U = L - Q$	0,9998	1,4565	1,4748
$\rho_O = U / C$	0,9998	0,7280	0,4916
$n = N - L$	66,6647	97,1029	98,3200
$\rho_{PC} = n / N$	0,6667	0,9710	0,9832
T_p	200,018	11,9343	6,8325
$T_Ц = T_p + t_{HO}$	600,018	41,9343	406,8325
ρ_{PC} / ρ_O	0,666	1,333	2

Контрольные вопросы и задания к главе 7

1. Перечислите основные понятия теории массового обслуживания.
2. Перечислите основные компоненты, входящие в состав системы массового обслуживания.
3. Поясните назначение дисциплины формирования очереди и дисциплины обслуживания очереди
4. Какие типы входящих потоков наиболее часто используют в СМО.
5. Перечислите и поясните основные свойства простейшего входящего потока.
6. По каким параметрам простейший входящий поток отличается от пуассоновского входящего потока.
7. Напишите и поясните назначение параметров экспоненциальной функции распределения интервалов времени обслуживания заявок в СМО.
8. Чем отличается экспоненциальное распределение времени обслуживания заявок в СМО от распределения Эрланга.
9. Перечислите параметры, которые влияют на пропускную способность СМО.
10. Поясните назначение унифицированной системы обозначений СМО.
11. Перечислите основные показатели оценки качества функционирования СМО.
12. Поясните различие между показателями и критериями оценки качества функционирования СМО.
13. Поясните различие между СМО с ожиданием и СМО с отказами.
14. Поясните особенности СМО, отображающей работу канала связи с помехами.
15. Поясните особенности СМО, отображающей работу службы ремонта и обслуживания компьютеров.

Литература к главе 7

Основная

Таха Х. Введение в исследование операций: пер. с англ. / Х. Таха. М.: Вильямс, 2007. 912 с.

Дополнительная

Ермаков В.И. Справочник по математике для экономистов /В.Е. Бармаумов, В.И. Ермаков, Н.Н. Кривенцова, А.С. Лебедев, В.И. Матвеев, Б.М. Рудык, Е.А. Силаева, О.К. Смагина. М.: ИНФРА-М, 2006. 464 с.

Фомин Г.П. Математические методы и модели в коммерческой деятельности. / Г.П. Фомин. М.: Финансы и статистика, 2009. 643 с.

Приложение 1

Обеспечение информационной безопасности АСОИиУ

Типовой процесс создания эффективной комплексной системы защиты компьютерной информации в АСОИиУ, обычно включает следующие этапы:

1. Анализ структуры АСОИиУ, выявление информационных ресурсов, подлежащих защите, ранжирование ресурсов по степени важности.
2. Анализ факторов, влияющих на уязвимость информационных ресурсов
3. Анализ каналов утечки компьютерной информации.
4 Разработка модели угроз информационной безопасности и оценка возможного ущерба от утечки информации, подлежащей защите.
5. Определение функций и требований к системе защиты информации
6. Выбор методов и средств защиты компьютерной информации
7. Выбор вариантов комплексной системы защиты информации в АСОИиУ, критериев их сравнения и оценка ожидаемой эффективности от внедрения каждого из этих вариантов.
8. Доработка вариантов системы защиты информации для достижения требуемых показателей качества функционирования АСОИиУ.
9. Определение технико-экономической оценки эффективности для каждого из сравниваемых вариантов комплексной системы защиты информации.
10. Выбор, обоснование и утверждение варианта структуры и технологии функционирования комплексной системы защиты информации в АСОИиУ.
11. Установка комплексной системы защиты информации
12. Обучение всех сотрудников, обеспечивающих процесс функционирования комплексной системы защиты информации АСОИиУ.
13. Разработка порядка и режима контроля комплексной системы защиты информации АСОИиУ
14. Разработка правил эксплуатации АСОИиУ с учетом требований комплексной системы защиты информации.
15 Определение мер ответственности должностных лиц за нарушение правил эксплуатации АСОИиУ.

Комплексная система защиты компьютерной информации включает организационно-технические, программно-технические и административно-правовые методы защиты.

Организационно-технические методы защиты информации предусматривают:

- создание перечня объектов защиты, в который обязательно должы быть включены все виды серверов, и режимы доступа к ним;
- создание специальных рабочих помещений (серверных комнат) для размещения серверов с конфиденциальной информацией;
- выполнение работ по защите помещений от электромагнитного излучения;
- организацию пропускного режима в помещения:
- организацию контроля и регистрацию использования носителей данных

Программно-технические методы защиты информации предназначены для предотвращения нарушения конфиденциальности, целостности и несанкционированного изменения данных, хранимых и обрабатываемых в автоматизированной информационной системе.

Разрешение доступа к данным осуществляется путем идентификации, аутентификации, адресации и авторизации пользователя автоматизированной информационной системы. Идентификация пользователя – это процедура проверки подлинности его регистрационного имени, аутентификация – установление его подлинности за счет использования пароля доступа, адресация – процедура проверки разрешенного по времени входа в сеть и адресов компьютеров, с которых этот вход разрешен, авторизация - процедура проверки полномочий и привилегий пользователя на предоставленные ему возможности по работе с информацией.

Административно-правовые методы защиты информации предполагают выполнение требований документов, разработанных государственными органами, а также разработку внутрифирменных регламентирующих документов по работе с конфиденциальной информацией.

В настоящее время следует выделить следующие пять уровней правового обеспечения защиты информации:

Первый уровень составляют международные договоры, к которым присоединилась Российская Федерация, а также федеральные законы России, например, Федеральный закон России от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Второй уровень составляют указы Президента РФ и постановления Правительства РФ. Например, Указ Президента РФ: от 6 марта 1997 года №188 «Об утверждении перечня сведений конфиденциального характера»;

Третий уровень составляют государственные стандарты (ГОСТы), касающиеся защиты информации, среди которых особо следует отметить следующие:

- ГОСТ Р 53114 - 2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».
- ГОСТ ИСО/ МЭК 15408-2002 «Общие критерии оценки безопасности информационных технологий», включающий три части;
- ГОСТ Р ИСО/МЭК 17799-2005. «Информационная технология. Практические правила управления информационной безопасностью»
- ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

Четвертый уровень составляют руководящие документы и методики, разработанные государственными органами. Среди них следует отметить набор руководящих и нормативно-методических документов от 25 июля 1997 года которые разработаны Гостехкомиссией (ГТК) России: при Президенте РФ, и посвящены вопросам защиты от несанкционированного доступа (НСД) к информации:

Пятый уровень составляют документы по защите информации в АСОИиУ, разработанные непосредственно в организации, которая осуществляет обслуживание, эксплуатацию и сопровождение этой системы.

К этим документам, в частности, относятся:

- устав организации, закрепляющий условия обеспечения ее деятельности по защите информации;
- перечень сведений, составляющих конфиденциальную информацию организации;
- положение о работе с конфиденциальной информацией;
- ответственность за нарушение режима работы с конфиденциальной информацией и ее разглашение;
- обязанности лиц, допущенных к работе с конфиденциальной информацией;
- правила эксплуатации автоматизированных информационных систем, содержащие порядок установки программного обеспечения на компьютеры; порядок подключения компьютеров к сети; правила доступа пользователей в сеть и правила работы с электронной почтой;
- должностные обязанности и права руководителей, специалистов и персонала, занятого обслуживанием автоматизированных информационных систем.

Приложение 2

Оценка рисков информационной безопасности

Риск – это предполагаемое событие, способное принести ущерб или убыток. Оценка риска информационной безопасности АСОИиУ– это процесс определения уровня ущерба или убытка в качественной или количественной форме, получаемого в процессе эксплуатации АСОИиУ за определенный период.

Для оценки рисков информационной безопасности разработано и широко используется в практической деятельности большое число методов и реализующих их программных продуктов. Все эти методы можно разделить на три группы:

- методы, использующие оценку риска на качественном уровне (например, риск оценивается по шкале «высокий», «средний», «низкий»);
- методы, использующие оценку риска на количественном уровне (риск оценивается через числовое значение, например, размер ожидаемых годовых потерь);
- методы, использующие смешанные оценки, т. е. первоначальные оценки даются на качественном уровне, а потом, используя вербально-числовые шкалы, производится их перевод в количественные оценки (в баллах).

Рассмотрим некоторые из этих методов, относящиеся к разным группам, и отражающие основные принципы и этапы оценки рисков информационной безопасности автоматизированных систем.

«Процесс упрощенного анализа рисков»

(Facilitated Risk Analysis Process - FRAP) для незащищенной системы

Метод FRAP предложен компанией Peltier and Associates. для оценки рисков информационной безопасности автоматизированных систем на качественном уровне. Основу метода составляет подход нахождения баланса между затратами на средства защиты и получаемым эффектом от использования этих средств.

Основные этапы оценки рисков при использовании метода FRAP могут быть представлены следующим образом:

Этап 1. Определение защищаемых ресурсов системы, обычно проводится экспертным методом с использованием опросных листов.

Этап 2. Идентификация и составление списка угроз, проводится экспертным методом с определением перечня наиболее вероятных угроз для рассматриваемых ресурсов системы.

Этап 3. Оценка уровня информационных угроз, который определяется как произведение вероятности возникновения угрозы на величину ущерба, который может быть нанесен данной угрозой при ее реализации..

При этом оценку вероятности возникновения угрозы и величины ущерба от ее реализации проводят по качественным шкалам («высокий», «средний», «низкий»).

Оценка уровня информационных угроз с использованием матрицы рисков приведена в табл П2.1

Таблица П2.1

Оценка уровня информационных угроз

Вероятность возникновения угрозы	Величина ущерба		
	Высокая	Средняя	Низкая
Высокая	A	B	B
Средняя	B	B	C
Низкая	B	C	D

При проведении анализа выделяют четыре уровня информационных угроз:

уровень А – информационная угроза носит недопустимый характер, поэтому внедрение системы защиты информации должно быть выполнено в обязательном порядке и немедленно;.

уровень В – информационная угроза носит средний характер, поэтому внедрение системы защиты информации должно быть выполнено по мере возможности, но в ближайшее время;

уровень С – информационная угроза носит допустимый характер, поэтому требуется провести мониторинг ситуации и по его результатам

принять решение о целесообразности принятия мер, противодействующих угрозе, и необходимости внедрения системы защиты информации;

уровень D – информационная угроза несущественна, поэтому в данный момент никаких действий по внедрению системы защиты информации, противодействующей данной угрозе, предпринимать не требуется.

Этап 4. Выбор варианта системы защиты информации в зависимости от проведенной оценки уровня информационной угрозы. Для оценки экономической эффективности выбранных средств защиты необходимо учитывать соотношение затрат на систему защиты информации и получаемого эффекта от ее внедрения. При этом обязательно следует учитывать не только стоимость системы защиты информации, но и стоимость ее эксплуатации.

Этап 5. Установка системы защиты информации и документирование результатов ее работы с целью их использования при формировании политики безопасности.

«Анализ рисков информационных систем»

(RiskWatch for Information Systems) компании RiskWatch,,

Этот метод предложен для оценки рисков информационной безопасности автоматизированных систем на количественном уровне.

В этом методе в качестве критериев используются:

- для количественной оценки рисков - ожидаемые годовые потери (Annual Loss Expectancy - ALE);
- для выбора варианта системы защиты информации - оценка возврата инвестиций (Return on Investment - ROI).

Метод компании RiskWatch ориентирована на количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты, чтобы система защиты приносила экономический эффект.

Метод «Анализ рисков информационных систем» состоит из четырех этапов.

На первом этапе определяют состав исследуемой системы и базовые требования в области ее безопасности. Для облегчения работы аналитиков имеется набор шаблонов, включающих списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты, из которого выбирают только нужные шаблоны.

На втором этапе осуществляют ввод данных в выбранные шаблоны, т. е. описывают конкретные характеристики ресурсов системы и потери, задают частоту возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов.

На третьем этапе проводят количественную оценку риска и выбирают меры обеспечения безопасности. Для этого сначала устанавливают связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих этапах. Риск для каждого ресурса оценивается в виде математического ожидания потерь за год, т.е. стоимость ресурса умножается на вероятность реализации угрозы для этого ресурса.. Например, если стоимость ресурса (сервера с информацией) составляет 100 тыс. руб, а вероятность того, что информация на нем будет уничтожена злоумышленником в течение года, равна 0.05, то ожидаемые потери на восстановление сервера составят 5 тыс. руб

Далее в величину ожидаемых потерь для каждого ресурса вводятся поправки в виде коэффициентов, показывающих сколько раз в год в среднем данная угроза реализуется в той части мира и в том месте, где установлена рассматриваемая автоматизированная система Эти поправки вводятся с учетом рекомендаций американского института стандартов (National Institute of Standards and Technology - NIST) Программное обеспечение компании RiskWatch имеет базы данных, содержащие наборы указанных коэффициентов.

После вычисления оценки риска информационной безопасности для каждого ресурса автоматизированной системы, проводится оценка риска

для всей автоматизированной системы, как сумма всех рисков отдельных ресурсов системы.

Программное обеспечение компании RiskWatch имеет базы данных, которые содержат обобщенные описания различных типов средств защиты и рекомендации по их использованию.

Эффект от внедрения средств защиты информации в автоматизированной системе количественно оценивается с помощью показателя возврат инвестиций ROI (Return on Investiment). Он показывает отдачу от инвестиций, сделанных в установку системы защиты информации в автоматизированную систему, за определенный период времени, и вычисляется по следующей формуле:

$$ROI = Z_c - Z_з$$

Где Z_c ожидаемое снижение потерь при эксплуатации автоматизированной системы за счет предотвращения угроз информационной безопасности, например, в руб;

$Z_з$ - затраты на установку и эксплуатацию системы защиты информации, например, руб.

На четвертом этапе проводят генерацию требуемых отчетов. Например, можно получить отчет о стоимости защищаемых ресурсов, ожидаемых потерях от реализации угроз ресурсам, отчет о ROI и т. д. Как правило, отчеты дают материал, достаточный для принятия решения о выборе варианта системы обеспечения информационной безопасности..

Метод «Анализ рисков информационных систем» (RiskWatch for Information Systems) и его программная реализация позволяют оценить не только возможные риски информационной безопасности, но и ту выгоду, которую может принести внедрение средств защиты информации.

«Анализ базовой проверки безопасности от Microsoft»

(Microsoft Baseline Security Analyzer- MBSA)

Метод реализован программно в виде продукта MBSA, анализатора базовой проверки безопасности и уязвимости, разработанного Microsoft, и предназначенного для администраторов, аудиторов безопасности и ИТ-специалистов. мелких и средних предприятий. MBSA позволяет оказать им помощь в определении состояния безопасности информационных систем, работающих под управлением ОС Microsoft, и предлагает конкретные рекомендации по улучшению безопасности этих систем.

MBSA позволяет найти типичные ошибки неверных настроек в конфигурации безопасности и выявить отсутствующие обновления безопасности для Windows, служб Internet Information Services (IIS), сервера SQL Server, обозревателя Internet Explorer и приложений Microsoft Office. проигрывателя Windows Media, сервера Exchange Server и т.д.

MBSA обеспечивает согласованность с другими продуктами Microsoft, такими, как центр обновлений Microsoft Update (MU), службы обновления Windows Server Update Services (WSUS), Systems Management Server (SMS), System Center Configuration Manager (SCCM) 2007 и Small Business Server (SBS).

Полный список продуктов, поддерживаемых MBSA, основанный на технологиях центра обновлений Microsoft и служб обновлений Windows Server Update Services (WSUS) можно найти на странице Продукты, поддерживаемые WSUS.

В практической деятельности используют MBSA 2.1, MBSA 2.2 и MBSA 2.3 (продукт рекомендован к использованию в январе 2015 года). С помощью MBSA нельзя проверить компьютер под управлением Windows 95, Windows 98 или Windows Millennium Edition.

MBSA 2.2, по сравнению с MBSA 2.1, отличают следующие особенности:

- добавлена поддержка Windows 7 и Windows Server 2008 R2;
- обновлен графический пользовательский интерфейс

- поддержка 64-разрядных платформ и проверок оценки уязвимости;
- улучшена поддержка проверок оценки уязвимости SQL Server 2005;
- добавлена новая функция для выдачи отчетов о законченных проверках по выбранному пользователем пути каталогов или общему сетевому ресурсу (функция командной строки /rd)
- совместимость с Windows Server Update Services 2.0 и 3.0

MBSA 2.3 , по сравнению с MBSA 2.2, отличают следующие особенности: добавлена поддержка Windows 8 и Windows 8.1, Windows Server 2012 , Windows Server 2012 R2.

Процесс оценки и управления рисками в информационных системах, предлагаемый корпорацией Майкрософт, включает три этапа.

На первом этапе осуществляется планирование и сбор следующих данных: активы, угрозы безопасности . уязвимости, меры защиты, элементы контроля

Активы организации – это все компоненты информационной системы, представляющие ценность для организации. Выделяют материальные активы, например, серверы, и нематериальные активам, например, информация, хранящаяся в цифровой форме на сервере.

Процесс управления рисками безопасности, предлагаемый корпорацией Майкрософт, определяет следующие три качественных класса активов, влияющих на бизнес:

1. высокое влияние на бизнес (ВВБ) - влияние на конфиденциальность, целостность и доступность этих активов может причинить организации значительный или катастрофический ущерб. Например, к этому классу относятся все конфиденциальные данные.
2. среднее влияние на бизнес (СВБ) - влияние на конфиденциальность, целостность и доступность этих активов может причинить организации средний ущерб, который не вызывает значительных изменений, но нарушает нормальную работу организации. К этому классу обычно

относятся все внутренние коммерческие данные, например, такие как перечень сотрудников, заказы предприятия.

3. низкое влияние на бизнес (НВБ) - это все активы, не попадающие в классы ВВБ и СВБ, например, общие сведения о структуре организации.

Далее определяется перечень угроз и уязвимостей, а затем выполняется оценка уровня потенциального ущерба, вызываемого степенью подверженности актива воздействию со стороны угрозы . Оценка ущерба актива предлагается проводить по следующей шкале:

- высокая подверженность актива воздействию угрозы, когда имеет место значительный или полный ущерб для актива;
- средняя подверженность актива воздействию угрозы, когда имеет место средний или ограниченный ущерб;.
- низкая подверженность актива воздействию угрозы, когда имеет место незначительный ущерб или ущерб практически отсутствует.

На втором этапе сначала проводится оценка частоты возникновения угроз. Различают: следующие оценки частот:

- высокая, когда вероятно возникновение угрозы в пределах года;
- средняя, когда влияние угрозы может возникнуть в пределах двух-трех лет;.
- низкая, когда возникновение влияния угрозы в пределах двух-трех лет маловероятно.

Данные собираются и заполняются в наборы шаблонов (в виде файлов Excel) для проведения дальнейшего анализа.

Для угроз указывается уровень их воздействия в соответствии с концепцией многоуровневой защиты (различают уровни - физический, сети, хоста, приложения, данных).

Для каждого актива составляется таблица типа табл. П2.3, в которой по вертикали указываются возможные классы актива (низкий –Н, средний –С, высокий- В), а по горизонтали возможные уровни подверженности актива воздействию угроз.(низкий –Н, средний –С, высокий- В)

Возможный уровень влияния угрозы на актив определяется с учетом значения класса актива и уровня подверженности актива воздействию и принимает значение, расположенное на пересечении соответствующих значений строки и столбца

Таблица П2.3

Возможный уровень влияния угрозы на актив

Классы активов	Уровень подверженности актива воздействию		
	Низкий	Средний	Высокий
Высокий	С	В	В
Средний	Н	С	В
Низкий	Н	Н	С

Уровни влияния угрозы на актив: Н – низкий, С – средний , В - высокий

Итоговый уровень риска актива определяется исходя из уровня влияния угрозы на актив и частоты возникновения угрозы, как показано в табл П2.4

Таблица П2.4

Итоговый уровень риска актива

Возможный уровень влияния угрозы на актив	Частота возникновения угрозы		
	Низкая	Средняя	Высокая
Высокий	С	В	В
Средний	Н	С	В
Низкий	Н	Н	С

Итоговый уровень риска актива: Н – низкий, С – средний , В - высокий

На третьем этапе создается упорядоченный по приоритетам список рисков активов. Сначала указываются активы, имеющие наибольший итоговый риск. Существенные риски активов детализируются и принимается решение о способах их минимизации

Приложение 3.
Основные системы массового обслуживания

Описания систем массового обслуживания (СМО) унифицированы и имеют следующий символьный вид: a/b/c/d/e/f

где символы a,b,c,d,e,f соответствуют конкретным и наиболее важным элементам представления процессов обслуживания заявок в СМО и интерпретируются следующим образом:

a – вид распределения интервалов времени между моментами поступления входящих в СМО заявок;

b - вид распределения времени обслуживания заявок в обслуживающем аппарате СМО;

c – количество обслуживающих аппаратов в СМО;

d – максимальное количество заявок, которое может одновременно находиться в очереди СМО;

e - дисциплина обслуживания заявок из очереди;

f - емкость источника, генерирующего заявки на обслуживание в СМО..

Для конкретизации символов a и b приняты следующие обозначения:

M – пуассоновское распределение моментов поступления входящего потока заявок на обслуживание или экспоненциальное распределение интервалов времени обслуживания заявок;

D – фиксированный (детерминированный) интервал времени между моментами последовательных поступлений заявок в систему на обслуживание или детерминированная продолжительность обслуживания;

E_K - распределение Эрланга интервалов времени между моментами последовательных поступлений заявок в систему или продолжительностей обслуживания, при этом K – это параметр распределения Эрланга;

GI – распределение произвольного вида моментов поступления заявок в систему на обслуживание;

G - распределение произвольного вида продолжительностей обслуживания заявок в обслуживающем аппарате системы.

Для конкретизации символа (c) указывается число от 1 до ∞;
Для конкретизации символа (d) указывается число от 1 до ∞;
Для конкретизации символа (e) приняты следующие обозначения:
ППП0 - первым пришел – первым обслужен; ОТН - относительные приоритеты; АБС - абсолютные приоритеты; КОМ - комбинированные приоритеты; ДБС - дообслуживание заявки при прерывании обслуживания; ЗАН - обслуживание заявки заново при прерывании обслуживания;
Для конкретизации символа (f) используют число 1, 2 , N, ∞; которое указывает емкость источника заявок

Для иллюстрации обозначения СМО рассмотрим пример.

Пример. Написать обозначение для СМО с пуассоновским входящим потоком, экспоненциальным распределением времени обслуживания, с одним ОА, с бесконечной емкостью буфера, с дисциплиной выбора заявок первый пришел - первым обслужен и с бесконечной емкостью источника заявок.

Решение. Рассматриваемая СМО имеет следующее обозначение:
M / M / 1 / ∞ / ППП0 / ∞.

Следует иметь в виду, что СМО, при описании которых последние три символа имеют вид ∞ / ППП0 / ∞., считают базовыми и эти последние три символа обычно опускают, а для обозначения таких СМО используют краткую форму записи, содержащую только первые три символа. Поэтому краткая форма обозначения рассматриваемой СМО имеет вид: M / M / 1

Для описания входных и выходных данных моделей СМО будем использовать следующие обозначения.

λ - интенсивность входящего потока заявок в СМО;

μ - интенсивность обслуживания заявок в ОА;

$t_0 = 1/\mu$ - среднее время обслуживания заявок в ОА;

с- число обслуживающих аппаратов, входящих в состав СМО;

$\rho = \lambda/(c \cdot \mu)$ - загрузка обслуживающего аппарата СМО;

$\varphi = \lambda / \mu$ - загрузка СМО, т.е. суммарная загрузка всех ОА;

m - число мест ожидания заявок в очереди СМО;

P_0 - вероятность простоя СМО, в СМО нет ни одной заявки;

P_i - вероятность, что в СМО, в очереди и на обслуживании, i - заявок;

P_{c+i} - вероятность, что заняты все «с» ОА и i - заявок в очереди;

P_W - вероятность ожидания заявкой начала обслуживания;

$P_{отк}$ - вероятность отказа заявке в обслуживании;

$\lambda_{отк}$ - интенсивность потока заявок, которым отказано в обслуживании

λ_c - интенсивность потока заявок, поступающих в СМО на обслуживание

U - коэффициент использования ОА для СМО с ограниченной очередью;

Q - среднее число заявок в очереди на обслуживание;

L - среднее число заявок в СМО, т. е. в очереди и на обслуживании;

W - среднее время нахождения заявок в очереди СМО;

T - среднее время пребывания заявок в СМО.

D_Q - дисперсия числа заявок в очереди СМО;

D_L - дисперсия числа заявок в СМО;

D_W дисперсия времени нахождения заявок в очереди СМО;

D_T - дисперсия времени пребывания заявок в СМО;

q - относительная пропускная способность СМО:

A - абсолютная пропускная способность СМО;

$P(t_{ож} < t)$ - вероятность, что время ожидания заявки в очереди меньше (t)

$P(t_{прб} < t)$ - вероятность, что время пребывания заявки в СМО меньше (t)

Показатели оценки качества функционирования СМО М/М/С

1. Загрузка обслуживающего аппарата СМО (ρ) и загрузка СМО (φ)

$$\rho = \frac{\varphi}{c} = \frac{\lambda}{c \cdot \mu} \quad \text{где } \rho < 1 \qquad\qquad \varphi = \frac{\lambda}{\mu} \quad \text{где } \varphi < c$$

2. Вероятность простоя СМО

$$P_0 = \left[\sum_{i=0}^{c} \frac{\varphi^i}{i!} + \frac{\varphi^{c+1}}{c! \cdot (c-\varphi)} \right]^{-1}$$

3 Вероятность, что в СМО i - заявок, где $i < c$

$$P_i = (\varphi^i / i!) P_0$$

4. Вероятность, что заняты все «с» ОА и i заявок в очереди

$$P_{c+i} = \frac{\varphi^{(c+i)}}{c^i \cdot c!} \cdot P_0$$

5. Вероятность ожидания заявкой начала обслуживания

$$P_W = 1 - \sum_{i=0}^{c-1} P_i = \frac{\varphi^c}{(c-1)! \cdot (c-\varphi)} \cdot P_0$$

6. Среднее число заявок в очереди СМО (Q) и в СМО (L)

$$Q = \sum_{i=c}^{\infty} (i-c) \cdot P_i = \frac{\varphi^{c+1} \cdot c \cdot P_o}{c! \cdot (c-\varphi)^2} \qquad\qquad L = Q + c \cdot \rho$$

7 Дисперсия числа заявок в очереди СМО (D_Q) и в СМО (D_L)

$$D_Q = \sum_{i=1}^{\infty} (i-1)^2 \cdot P_i - Q^2 \qquad\qquad D_L = \sum_{i=1}^{\infty} i^2 \cdot P_i - L^2$$

8. Среднее время нахождения заявок в очереди СМО (W) и в СМО (T)

$$W = \frac{Q}{\lambda} \qquad\qquad T = \frac{L}{\lambda} = W + \frac{1}{\mu}$$

9. Дисперсия времени нахождения заявок в очереди СМО

$$D_W = \sum_{i=1}^{\infty} i^2 \cdot P_i \cdot (\frac{1}{\mu})^2 - W^2$$

10. Дисперсия времени пребывания заявок в СМО

$$D_T = \sum_{i=1}^{\infty} (i+1)^2 \cdot P_i \cdot (\frac{1}{\mu})^2 - T^2$$

11 Вероятность, что время ожидания заявки в очереди меньше (t)

$$P(t_{ож} < t) = 1 - \rho \cdot e^{-(c\mu - \lambda) \cdot t}$$

12. Вероятность, что время пребывания заявки в СМО меньше (t)

$$P(t_{прб} < t) = 1 - e^{-(c\mu - \lambda) \cdot t}$$

Показатели оценки качества функционирования СМО M/M/C/m

1. Загрузка обслуживающего аппарата СМО $\rho = \frac{\varphi}{c} = \frac{\lambda}{c \cdot \mu}$

2. Загрузка СМО $\varphi = \frac{\lambda}{\mu}$

3. Вероятность простоя СМО $P_0 = \left[\sum_{i=0}^{c-1} \frac{\varphi^i}{i!} + \frac{\varphi^c (1-\rho^{m+1})}{c! \cdot (1-\rho)} \right]^{-1}$

4. Вероятность, что в СМО, i - заявок

$P_i = \frac{\varphi^i}{i!} P_0$ где $1 \le i \le c$ и $P_i = \frac{\varphi^i}{c! \cdot c^{i-c}} P_0$ где $c \le i \le (c+m)$

5. Вероятность отказа заявкам в обслуживании $P_{отк} = P_{m+c} = \frac{\varphi^{c+m}}{c! \cdot c^m} P_0$

6. Интенсивность потока заявок, поступающих в СМО на обслуживание

$$\lambda_c = (1 - P_{отк}) \cdot \lambda$$

7. Коэффициент использования ОА для СМО с ограниченной очередью

$$U = \lambda_c / (c \cdot \mu) = (1 - P_{отк}) \cdot \rho$$

8. Среднее число заявок в очереди на обслуживание

$$Q = \sum_{i=c+1}^{c+m} (i-c) \cdot P_i = \frac{\varphi^{c+m}}{c! \cdot c} \left[\frac{1 - \rho^m \left[(m+1) - m\rho \right]}{(1-\rho)^2} \right] P_0$$

9. Среднее число заявок в СМО, в очереди и на обслуживании

$$L = \sum_{i=1}^{c+m} i \cdot P_i = Q + c \cdot U$$

10. Среднее время нахождения заявок в очереди СМО

$$W = \frac{Q}{\lambda_c} = \frac{\varphi^c}{c! \cdot c \cdot \mu} \left[\frac{1 - \rho^m \left[(m+1) - m\rho \right]}{(1-\rho)^2} \right] P_0$$

11. Среднее время пребывания заявок в СМО $T = \frac{L}{\lambda_c}$

12. Относительная пропускная способность СМО $q = (1 - P_{отк})$

13. Абсолютная пропускная способность СМО $A = q \cdot \lambda$

Показатели оценки качества функционирования СМО M/M/1 и M/M/2

№	СМО M/M/1	СМО M/M/2
1	Загрузка обслуживающего аппарата	
	$\rho = \lambda / \mu$	$\rho = \lambda /(2 \cdot \mu)$
2	Вероятность простоя обслуживающего аппарата	
	$P_0 = 1 - \rho$	$P_0 = (1-\rho)/(1+\rho)$
3	Вероятность, что в СМО, i - заявок	
	$P_i = P_0 \cdot \rho^i$	$P_i = (\varphi^i / 2^i i!) P_0$ если i = 1,2 $P_i = \frac{\varphi^i}{2^i \cdot 2!} \cdot P_0$ если i = 3,4,5...
4	Среднее число заявок в очереди на обслуживание	
	$Q = \frac{\rho^2}{1-\rho}$	$Q = \frac{2 \cdot \rho^3}{1-\rho^2}$
5	Среднее число заявок в СМО , в очереди и на обслуживании	
	$L = \frac{\rho}{1-\rho}$	$L = \frac{2 \cdot \rho}{1-\rho^2}$
6	Дисперсия числа заявок в очереди СМО	
	$D_Q = \frac{\rho^2(1+\rho-\rho^2)}{(1-\rho)^2}$	$D_Q = \frac{2\rho^3(1+2\rho-\rho^3)}{(1-\rho^2)^2}$
7	Дисперсия числа заявок в СМО	
	$D_L = \frac{\rho}{(1-\rho)^2}$	$D_L = \frac{2\rho \cdot (1+\rho^2)}{(1-\rho^2)^2}$
8	Среднее время нахождения заявок в очереди СМО	
	$W = \frac{\rho}{(1-\rho) \cdot \mu}$	$W = \frac{\rho^2}{(1-\rho^2) \cdot \mu}$
9	Среднее время пребывания заявок в СМО	
	$T = \frac{1}{(1-\rho) \cdot \mu} = \frac{1}{(\mu - \lambda)}$	$T = \frac{1}{(1-\rho^2) \cdot \mu}$

Показатели оценки качества функционирования СМО M/M/1/m

№	Показатель СМО
1	Загрузка обслуживающего аппарата $\rho = \lambda / \mu$
2	Вероятность простоя обслуживающего аппарата $P_0 = \frac{(1-\rho)}{(1-\rho^{m+2})}$
3	Вероятность, что в СМО, i - заявок $P_i = \frac{(1-\rho)\cdot\rho^i}{(1-\rho^{m+2})}$
4	Вероятность отказа заявкам в обслуживании $P_{отк} = P_{m+1} = \frac{(\rho^{m+1}-\rho^{m+2})}{(1-\rho^{m+2})}$
5	Интенсивность потока обслуженных заявок $\lambda_c = (1-P_{отк})\cdot\lambda$
6	Коэффициент использования обслуживающего аппарата $U = \lambda_c / \mu = (1-P_{отк})\cdot\rho$
7	Среднее число заявок в очереди на обслуживание $Q = \frac{\rho^2\cdot\left[1-\rho^m\cdot(m+1)+m\cdot\rho^{m+1}\right]}{(1-\rho^{m+2})\cdot(1-\rho)}$
8	Среднее число заявок в СМО $L = Q+U = \frac{\rho\cdot\left[1-(m+2)\rho^{m+1}+(m+1)\cdot\rho^{m+2}\right]}{(1-\rho^{m+2})\cdot(1-\rho)}$
9	Среднее время нахождения заявок в очереди СМО $W = \frac{Q}{\lambda_c} = \left[\frac{\rho}{(1-\rho)} - \frac{(m+1)\cdot\rho^{m+1}}{(1-\rho^{m+1})}\right]\cdot\frac{1}{\mu}$
10	Среднее время пребывания заявок в СМО $T = \frac{L}{\lambda_c} = \left[\frac{1}{(1-\rho)} - \frac{(m+1)\cdot\rho^{m+1}}{(1-\rho^{m+1})}\right]\cdot\frac{1}{\mu}$

Показатели оценки качества функционирования СМО M/M/2/m

№	Показатель СМО
1	Загрузка обслуживающего аппарата $\rho = \frac{\varphi}{2} = \frac{\lambda}{2\mu}$
2	Вероятность простоя обслуживающего аппарата $P_0 = \frac{(1-\rho)}{(1+\rho-2\rho^{m+3})}$
3	Вероятность, что в СМО, i - заявок $P_i = 2 \cdot \rho^i \cdot P_0$
4	Вероятность отказа заявкам в обслуживании $P_{отк} = P_{m+2} = \frac{(2\rho^{m+2} - 2\rho^{m+3})}{(1+\rho-2\rho^{m+3})}$
5	Интенсивность потока обслуженных заявок $\lambda_C = (1-P_{отк}) \cdot \lambda = \frac{(1+\rho-2\rho^{m+2})}{(1+\rho-2\rho^{m+3})} \cdot \lambda$
6	Коэффициент использования обслуживающего аппарата $U = \lambda_c / 2\mu = (1-P_{отк}) \cdot \rho$
7	Среднее число заявок в очереди на обслуживание $Q = \frac{2 \cdot (m \cdot \rho^{m+4} - m \cdot \rho^{m+3} - \rho^{m+3} + \rho^3)}{(1-\rho) \cdot (1+\rho-2\rho^{m+3})}$
8	Среднее число заявок в СМО $L = Q + 2U = \frac{2-2(m+3) \cdot \rho^{m+2} + 2(m+2) \cdot \rho^{m+3}}{(1-\rho) \cdot (1+\rho-2\rho^{m+3})} \cdot \rho$
9	Среднее время нахождения заявок в очереди СМО $W = \frac{Q}{\lambda_C} = \frac{m\rho^{m+3} - m\rho^{m+2} - \rho^{m+2} + \rho^2}{(1-\rho) \cdot (1+\rho-2\rho^{m+2}) \cdot \mu}$
10	Среднее время пребывания заявок в СМО $T = \frac{L}{\lambda_C} = \frac{(m+2)\rho^{m+3} - (m+3)\rho^{m+2} + 1}{(1-\rho) \cdot (1+\rho-2\rho^{m+2}) \cdot \mu}$

Показатели оценки качества функционирования СМО типа M/M/1/m и M/M/2/m при $\rho = 1$

№	СМО M/M/1/m	СМО M/M/2/m
1	Вероятность отказа заявкам в обслуживании	
	$P_{отк} = 1/(m+2)$	$P_{отк} = 2/(2m+5)$
2	Коэффициент использования обслуживающего аппарата	
	$U = \frac{(m+1)}{(m+2)}$	$U = \frac{(2m+3)}{(2m+5)}$
3	Интенсивность потока обслуженных заявок	
	$\lambda_c = \frac{(m+1)}{(m+2)} \cdot \lambda$	$\lambda_c = \frac{(2m+3)}{(2m+5)} \cdot \lambda$
4	Среднее число заявок в очереди на обслуживание	
	$Q = \frac{m \cdot (m+1)}{2 \cdot (m+2)}$	$Q = \frac{m \cdot (m+1)}{(2m+5)}$
5	Среднее число заявок в СМО	
	$L = \frac{(m+1)}{2}$	$L = \frac{(m+2) \cdot (m+3)}{(2m+5)}$
6	Среднее время нахождения заявок в очереди СМО	
	$W = \frac{m}{2 \cdot \mu}$	$W = \frac{m \cdot (m+1)}{(2m+3) \cdot \mu}$
7	Среднее время пребывания заявок в СМО	
	$T = \frac{(m+2)}{2 \cdot \mu}$	$T = \frac{(m+2) \cdot (m+3)}{(2m+3) \cdot 2 \cdot \mu}$
8	Относительная пропускная способность СМО	
	$q = \frac{(m+1)}{(m+2)}$	$q = \frac{(2m+3)}{(2m+5)}$
9	Абсолютная пропускная способность СМО	
	$A = \frac{(m+1)}{(m+2)} \cdot \lambda$	$A = \frac{(2m+3)}{(2m+5)} \cdot \lambda$

Приложение 4

Основные термины в области администрирования и развития АСОИиУ

Авторизация пользователя - проверка полномочий пользователя на доступ к конкретным ресурсам автоматизированной системы с целью разграничения прав доступа к этим ресурсам

Администратор базы данных – специалист, отвечающий за разработку требований к базе данных, её проектирование, реализацию, эффективное использование и сопровождение, включая управление учётными записями пользователей базы данных, защиту данных от несанкционированного доступа, а также поддержку целостности базы данных.

Администрирование базы данных – процесс управления работой базы данных в процессе промышленной эксплуатации системы.

Администрирование системы - планирование, установка, управление конфигурацией, обслуживание и сопровождение аппаратно-программных средств автоматизированных систем.

Администрирование сервера системы:- управление конфигурацией сервера, создание пользователей, организация защиты данных, резервное копирование и обеспечение нормальной работы всех приложений.

Альтернативный вариант развития системы - один из нескольких возможных вариантов развития системы, соответствующий установленным критериям выбора.

Аутентификация пользователя - установление подлинности пользователя путем сравнения введенного им пароля (секрета) с паролем, хранимым в базе данных пользователей.

База данных — совокупность логически связанных данных, используемых прикладными программами для удовлетворения информационных потребностей пользователей, хранимых на сервере и организованных в соответствии с концептуальной структурой, описывающей характеристики этих данных и взаимоотношения между ними.

Безотказность данных — свойство системы непрерывно сохранять набор данных в работоспособном состоянии, при котором она способна выполнять заданные функции с параметрами, установленными требованиями технической документации, за счет использования средств защиты данных от несанкционированного доступа и средств отказоустойчивости.

Документация на систему – набор документов, который обеспечивает идентификацию системы и измерительного оборудования, проверяемость работоспособности системы, оценку ее качества, разрешает и предупреждает спорные вопросы.

Защита информации – комплекс технических и организационных мероприятий, направленных на обеспечение информационной безопасности.

Идентификация пользователя – процедура проверки регистрационного имени пользователя.

Информационная безопасность автоматизированной системы - это защищенность данных и поддерживаемой инфраструктуры от случайных или непреднамеренных воздействий различного характера.

Конфиденциальность информации - это обеспечение доверительности использования информации и предотвращение ее утечки и разглашения

Метод Дельфи – метод комплексного анализа альтернативных вариантов развития системы, проводимый группой высококвалифицированных в данной области специалистов с применением экспертных оценок.

Метод экспертных оценок - метод сбора данных путем опроса экспертов.

Метод экспертного анализа – метод обработки экспертных оценок.

Мера риска - показатели, характеризующие уровень риска, для оценки меры риска используют следующие показатели: размах вариации, дисперсию, среднее квадратическое отклонение, коэффициент вариации.

Обслуживание и сопровождение автоматизированной системы - проведение диагностики системы, устранение отказов и сбоев в работе системы, восстановление работоспособности системы, замена неисправных компонентов и обеспечение эффективного режима ее функционирования.

Операцио́нная систе́ма — комплекс управляющих и обрабатывающих программ, которые, с одной стороны, выступают как интерфейс между устройствами вычислительной системы и прикладными программами, а с другой стороны предназначены для управления вычислительными процессами, распределения ресурсов между ними и организации надёжных вычислений.

Опытная эксплуатация системы – комплексная проверка правильности функционирования технических средств, программного обеспечения и технологического процесса обработки данных, в процессе которой в рабочий журнал заносят все сведения об отказах, сбоях, аварийных ситуациях и изменениях в настройке параметров, для обеспечения в будущем эффективной работы системы в реальных условиях.

Пароль — это набор символов, предназначенный для подтверждения личности или полномочий пользователя и защиты информации от несанкционированного доступа.

Политика информационной безопасности – это набор правил и рекомендаций по организации защиты информации в автоматизированной системе, который утверждается руководством организации.

Принятие решения - процесс анализа, оценки ситуации и выбора наилучшего варианта решения среди сравниваемых вариантов.

Программа и методика испытаний – документ, который устанавливает необходимый и достаточный объем испытаний, обеспечивающий заданную достоверность получаемых результатов, позволяющих судить о соответствии системы требованиям технического задания, разрабатывается на автоматизированную систему в целом и на ее отдельные компоненты, может включать тесты и контрольные примеры.

Промышленная эксплуатация системы – эксплуатация системы в реальных условиях ее применения после успешного проведения предварительных испытаний, опытной эксплуатации и приемо-сдаточных испытаний, утвержденных актом сдачи системы в эксплуатацию.

Работоспособность системы — это состояние системы, при котором она способна выполнять заданные функции с параметрами, установленными требованиями технической документации в течение определенного времени.

Ранг - порядковый номер альтернативного варианта развития системы, расположенный по возрастанию или убыванию предпочтений сравниваемых вариантов.

Ранговая оценка – оценка в виде ранга, выданная экспертом предлагаемому варианту развития системы, с учетом сравнения его по всем параметров с остальными альтернативными вариантами.

Реестр (или системный реестр**)** — иерархически построенная база данных параметров и настроек в большинстве операционных систем, которая содержит полную информацию о всех настройках аппаратного и программного обеспечения, а также профили пользователей.

Риск — это возможность возникновения неблагоприятной ситуации или неудачного исхода в производственной деятельности организации или работе оборудования. Часто считают, что риск — это произведение вероятности возникновения неблагоприятной ситуации на убыток от ее реализации.

Се́рвер — аппаратно- программный комплекс, в котором программное обеспечение принимает запросы от клиентов и их обрабатывает.

Сервер баз данных - выполняет обслуживание и управление базой данных и отвечает за целостность и сохранность данных, а также обеспечивает операции ввода-вывода при доступе клиентов к информации.

Сетевая операционная система — операционная система с возможностью работы компьютеров в сетях, позволяющая осуществлять поддержку сетевого оборудования и сетевых протоколов, а также поддержку доступа к удалённым ресурсам по сети и позволять удалённым пользователям использовать ресурсы сети.

Систе́мный администра́тор— сотрудник, должностные обязанности которого подразумевают обеспечение штатной работы аппаратного и

программного обеспечения сети, а также обеспечение информационной безопасности и защиты конфиденциальной информации.

Систе́ма управле́ния ба́зами да́нных (СУБД) — совокупность программных средств предназначенных для создания и поддержки баз данных, а также получения к ним контролируемого доступа.

Тестирование – это выявление и устранение возможных неисправностей в работе аппаратно-программных средств системы как на стадии ввода в опытную эксплуатацию, так и в процессе промышленной эксплуатации.

Управление риском защиты данных – выбор уровня защиты и оптимальных по цене мер и средств защиты, которые сокращают риск до допустимого уровня.

Уровень риска (степень риска) - характеризует уровень финансовых потерь организации от неблагоприятных условий; как правило, выделяют три уровня: минимальный, допустимый, недопустимый

Файловый сервер — это сервер, предназначенный для выполнения запросов клиентов по реализации файловых операций ввода-вывода и хранящий файлы на дисках, которые реализованы в виде отказоустойчивых дисковых массивов уровней RAID,. для обеспечения бесперебойной работы системы и увеличения скорости записи и чтения данных.

Экспертный метод анализа - проведение экспертами анализа проблемы с количественной оценкой суждений и формализованной обработкой полученных результатов.

Эксплуатация автоматизированных систем - комплекс технических и организационных мер по обеспечению взаимодействия пользователей и обслуживающего персонала со средствами вычислительной техники и правильному обращению с установленным на аппаратных средствах системным и прикладным программным обеспечением.