ПОСТРОЕНИЕ ЭЛЕКТРОННЫХ ХРАНИЛИЩ ДОКУМЕНТАЦИИ БОЛЬШИХ СИСТЕМ

ПЕРСПЕКТИВНЫЕ МЕТОДЫ И СРЕДСТВА

В.Г. Журавский, д. т. н.
В.В. Гольдин, к. т. н.

В процессе автоматизации крупные корпорации и госструктуры сталкиваются с необходимостью объединить информационные системы различного назначения. При этом обязательным шагом является создание центров хранения информации. Задача построения корпоративных электронных архивов объединяет технологии электронного документооборота, информационной поддержки жизненного цикла изделий, создания хранилищ аналитической информации. В данной статье обозначены общие тенденции, а также предложены конкретные методы развития центров хранения информации.

Правовой основой существования электронной документации является Федеральный закон об электронной цифровой подписи и ряд государственных стандартов, уравнивающих права традиционной и электронной формы документов [1,2]. На многих предприятиях электронные архивы в некотором виде уже созданы и функционируют. Они многократно упрощают учет, хранение и обработку документов. Однако эффективное функционирование таких хранилищ невозможно без интеграции с системами делопроизводства, электронного документооборота инженерно-конструкторских подразделений и т.д. В крупных корпорациях ведется архив проектов, где накапливается информация о всех этапах жизненного цикла системы (конкретного изделия). Поэтому пользователю требуется доступ к разнородным данным (технические, организационно-распорядительные документы и т.д.) с множественными логическими связями. Документы могут иметь несколько версий, соответствующих, например, различным стадиям разработки изделия. При построении хранилища нужно обеспечить и автоматическое внесение большого объема изменений в документацию. С точки зрения удаленного доступа эффективными являются глобальные виртуальные хранилища с применением порталов: через единый веб-интерфейс пользователи взаимодействуют как с корпоративным архивом, так и с СУБД отдельных ИТ-подразделений.

ОРГАНИЗАЦИЯ ХРАНИЛИЩА ЭЛЕКТРОННЫХ ДАННЫХ

Очевидные преимущества централизованного хранения электронной документации: поддержка любых форматов данных (чертежей, схем, таблиц, текстов, графических образцов), контроль продвижения документов по стадиям жизненного цикла (временное и постоянное хранение, контроль сроков хранения), удобный механизм навигации по структуре архива и т.д. Современные хранилища организованы в виде распределенной вычислительной структуры на основе проводных и беспроводных сетей передачи данных. Структура обычно включает центральную базу данных (БД), предназначенную для накопления и долгосрочного хранения информации, и сети локальных БД, интегрированных с системами информационной поддержки производственных процессов (разработки, изготовления, эксплуатации, и др.) как всей корпоративной системы, так и ее компонентов [3]. Кроме того, в состав хранилища входят подсистемы ввода (программно-аппаратные средства сканирования и индексирования документов) и тиражирования информации, резервного копирования (средства репликации данных), управления и обеспечения информационной безопасности хранилища (сбор статистики, журналирование, управление жизненным циклом документов).

В качестве среды обмена данными следует использовать локальные вычислительные сети, например сеть хранения SAN (Storage Area Network) [4]. SAN объединяет серверы с устройствами хранения информации со скоростью до 2 Гбайт/с. Общая структура сети (рис.1) включает: хост-адаптеры (HBA), дисковые массивы, устройства коммутации. Транспортной основой SAN является протокол Fiber Channel. Он поддерживает как медные (на расстоянии до 25 м), так и волоконно-оптические соединения (до 10 км). Проектирование кабельной сети осуществляется по правилам Gigabit Ethernet. Вместо традиционных шинных соединений сервера с устройствами хранения топология Fiber Channel предполагает соединения

точка-точка, петля с арбитражем (Arbitrated Loop, FC-AL), и через устройства коммутации.

Инфраструктура SAN включает концентраторы (Fibre Channel Hub), коммутаторы (Fibre Channel switch) и маршрутизаторы (Fibre Channel-SCSI router). Концентраторы объединяют устройства, работающие в режиме Arbitrated Loop. При такой топологии передающее устройство вначале инициализирует арбитраж за право использования среды передачи данных от узла к узлу. Устройства можно добавлять/отключать без остановки системы, так как концентратор автоматически размыкает/замыкает петлю. Однако каждое изменение структуры сети сопровождается многоступенчатым процессом инициализации, во время которого данные не передаются. Коммутаторы соединяют устройства по протоколу Fibre Channel и разграничивают зоны их доступа (Zone). Для устройств, помещенных в разные зоны, обмен данными невозможен. Коммутаторы по функциональности делятся на два типа. Из коммутаторов начального уровня невозможно составить модульную структуру или же они поддерживают связь только с одним таким же устройством. Коммутаторы второго типа объединяют в группы для увеличения числа портов. Они характеризуются резервированием основных узлов (блоков питания, процессоров, модулей коммутации) и большим числом портов (64 и более).

Для передачи данных от серверов (почтовых, веб- или серверов локальных СУБД) к устройствами SAN по протоколу Fibre Channel служат хост-адаптеры. Они устанавливаются в серверы и поддерживают большинство открытых платформ и шинных архитектур. В функции серверного ПО (драйверы, менеджеры томов) входит координация работы SAN, а именно:

- резервирование путей доступа серверов к дисковым массивам и динамическое распределение нагрузки между ними (поддержка таблиц путей доступа, отключение путей в случае сбоев и подключение новых с перераспределением нагрузки);
- резервное копирование данных хранилища, например перенос информации с дисковых массивов на ленточные библиотеки. При этом формируется таблица соответствия физических дисковых блоков логическим структурам данных для сохранения целостности их образа на ленте;
- управление зонами доступа через коммутаторы, обнаружение отказов, сбор статистики и т.д.

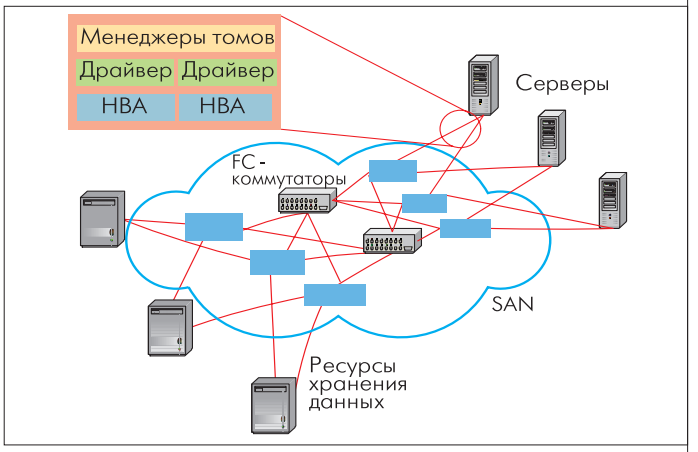

Рис.1. Общая структура и компоненты SAN

При использовании ленточных библиотек для долгосрочного хранения данных дисковые массивы служат для репликации данных по сети, и информация с них может поступать на ленту, минуя сеть и серверы. В конфигурации SAN заложены возможности (рис.2) подключения новых дисковых массивов и серверов без остановки системы.

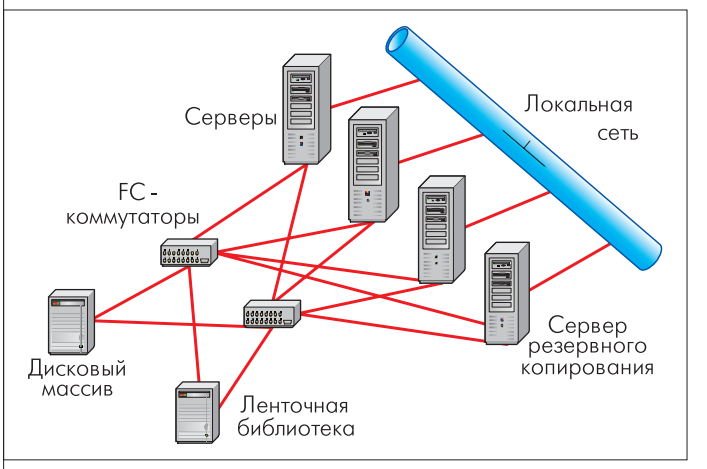

Рис.2. Полномасштабная SAN центрального хранилища

ПОВЫШЕНИЕ ОТКАЗОУСТОЙЧИВОСТИ СЕТИ ХРАНЕНИЯ ДАННЫХ

Такая структура сети позволяет строить надежные крупномасштабные хранилища. Основные средства повышения стабильности их работы – аппаратная избыточность и создание страховочных копий информации. Обычно наряду с основным хранилищем создают резервное, соединив их по протоколу Fiber-Channel, для асинхронной и синхронной репликации данных. Таким образом, благодаря прямому доступу центров хранения к дисковым массивам и ленточным библиотекам друг друга, информация в них одинаково актуальна. Кроме того, в SAN следует использовать две независимые группы коммутаторов. Тогда система сохранит работоспособность в случае отказа оборудования, изменения конфигурации или установки программно-аппаратных средств на одной из групп.

Отказоустойчивость хранилища зависит и от выбора дисковой подсистемы. Следует применять диски с большим временем наработки на отказ, электронные компоненты проверенных производителей и т.д. Повсеместной практикой является использование избыточных RAID-массивов дисков для хранения оперативной информации и метаданных.

Дисковые носители также следует дублировать. Резервное копирование – обязательная часть политики хранения электронных данных. RAID-массивы позволяют обрабатывать данные в случае неисправности одного из дисков, входящих в массив. Но они не гарантируют логическую целостность данных в случае алгоритмических ошибок, программных сбоев или некорректных действий пользователей. Человеческий фактор обычно приводит к удалению нужной информации без возможности восстановления. Также повреждения наносят компьютерные вирусы, которые преднамеренно портят или удаляют программы и данные. С точки зрения RAID-контроллера, их действия правомерны, так как происходят обычные операции чтения/записи, поэтому единственный гарант сохранности данных – резервная копия. Чем свежее и полнее копия, тем выше шансы на восстановление. Желательно иметь не менее двух резервных копий, различающихся по дате. В некоторых случаях может оказаться полезной и не самая последняя запись, например если какие-то из файлов попали в резерв уже зараженные вирусом. То же относится к случаю, когда после выполнения операций над данными сохранены только результаты. Если исходные данные нужно обработать по-другому, их восстанавливают из резервной копии.

Правильный выбор схемы резервного копирования (рис.3) позволяет восстановить данные практически любой давности. Критерий успешности такой системы – автоматическое выполнение резервного копирования в назначенное время суток и восстановление важной информации при аварийных ситуациях в кратчайшие сроки. Сохраняются как данные, создаваемые пользователями хранилища при работе с ПО, так и сами приложения. Обычно резервное копирование применяется к серверам БД и электронной почты, данным аналитической обработки сетевой СУБД. Проведение резервного копирования информации на рабочих станциях пользователей хранилища уменьшает риски, связанные с непреднамеренными ошибками, умышленными действиями или неполадками оборудования. Копии хранятся на специализированном отказоустойчивом устройстве. На сервере резервного копирования происходит обработка потока данных, журналирование транзакций. Для оптимизации процесса резервирования удаленных серверов и уменьшения сетевого трафика применяют сжатие и распределенную обработку данных.

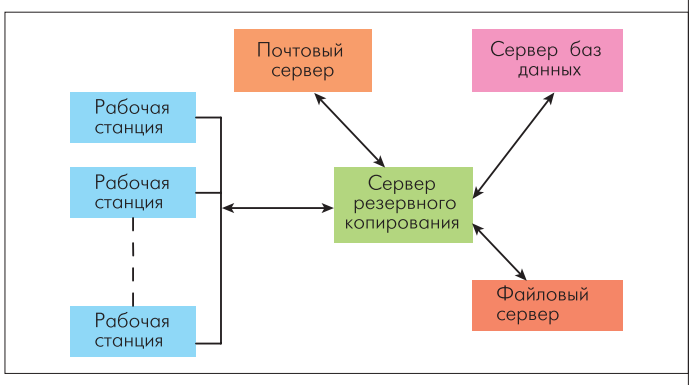

Рис.3. Структура системы резервного копирования

Еще один способ повышения отказоустойчивости – кластерная организация вычислительного процесса [5]. Кластеры состоят как минимум из двух узлов и разделяемого дискового пространства. Они поддерживают динамическое перераспределение нагрузки между узлами. Время простоя оборудования, вызванное, например, профилактическим обслуживанием, сводится к минимуму – ресурсы одного из узлов в плановом порядке переводятся на другие без ущерба для всей системы. Кластеры с минимальной конфигурацией обычно предоставляют приемлемый уровень отказоустойчивости (работоспособны в течение 85–90% времени). Коэффициент готовности структуры из трех узлов уже достигает 99,99%, то есть за год по причине сбоев и аппаратных неполадок оборудование простаивает примерно 55 минут.

ЛОГИЧЕСКАЯ СТРУКТУРА ХРАНИЛИЩА

Кроме надежности и производительности сети хранения, важна и функциональность логической структуры хранилища. В качестве базовой обычно принимают структуру в виде иерархии папок, вложенность которых отражает логическую связь узлов системы. Помимо интуитивно понятной навигации (пользователь представляет, где искать нужный документ) подобная организация архива облегчит интеграцию со специализированным ПО обработки данных. Однако в случае развитой структуры цепочка вложенных папок, по которой можно найти документ, не известна. Поэтому хранилища предусматривают возможность атрибутивного или полнотекстового поиска. Атрибутивный поиск производится по признакам, предназначенным для классификации, идентификации и быстрого поиска документа. Они являются частью служебных метаданных, полученных при индексировании документа и сопровождающих его в архиве. Во втором случае в качестве поискового образа используется весь текст документа, учитываются результаты морфологического и лексического анализа. При полнотекстовом поиске обязательным этапом добавления документа в архив является распознавание и верификация текста.

Средства ввода электронных документов должны быть интегрированы со средствами формирования самих документов: устройствами сканирования бумажных носителей и микрофишей*, импорта электронных документов из сущес-

* Микрофиша – фотодокумент на прозрачной пленке с последовательным расположением кадров в несколько рядов.

твующих хранилищ или внешних источников. Желательно, чтобы пользователь мог сохранить документ в архив непосредственно из того приложения, в котором он его создает. Требования ПО для обработки документов также должны быть учтены. Например, при сканировании графических образцов необходимо автоматически выбирать соответствующее разрешение и формат электронного представления. С развитием информационных и телекоммуникационных технологий перспективными направлениями становятся сканирование информации с материальных предметов с применением трехмерных сканеров, поддержка геоинформационных запросов, логическая обработка информации на основе причинно-следственных связей и т.д.

Помимо простого формирования иерархических списков электронных документов удобно использовать виртуальные документы (электронные подшивки), устанавливая и динамически отслеживая логические связи между объектами хранилища. В виртуальные документы можно объединять компоненты различных форматов. Связь между объектами фиксируется в момент регистрации документа в хранилище и ассоциируется с его текущей версией. Автоматически фиксируется связь и с новыми версиями объектов, входящих в подшивку. Один документ может входить в несколько виртуальных, а его замена и обновление производятся одновременно в каждом из них. В то же время каждый компонент сохраняет самостоятельность доступа, набор атрибутов, список авторизованных пользователей. То есть несколько пользователей могут одновременно работать с разными частями виртуального документа. При создании виртуальных документов многоуровневой вложенности связь между компонентами может быть иерархической. Это существенно оптимизирует работу с хранилищем. Например, выполнять операции над всеми компонентами подшивки можно обратившись только к корневому документу.

Также для упрощения и унификации средств доступа к архиву, целесообразно использовать Web-интерфейс приложения-навигатора. С помощью технологии порталов пользователи могут создавать, находить и редактировать документы из знакомой им программной среды. Архитектурно порталы состоят из набора "портлетов" (активных веб-элементов) – шлюзов к различным прикладным программам, например локальным СУБД. Таким образом через Web-приложения предоставляется одновременный доступ к распределенным хранилищам и различные функции обработки информации, адаптированные под конкретного пользователя.

СРЕДСТВА ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ЖИЗНЕННОГО ЦИКЛА ДОКУМЕНТОВ

Современная тенденция – самостоятельная работа исполнителя в рамках распределенных рабочих коллективов. При этом важно обеспечить разносторонние производственные связи исполнителей друг с другом. В крупных организациях хранилище электронной документации является не только местом размещения информации, но и единой средой обработки. Организация работы с документами определяется средствами автоматизации производственных процессов Work Flow. Между участниками коллектива, согласно набору процедурных правил, передаются не только данные, но и задания, связанные с их обработкой. Также системы Work Flow устанавливают маршрут документа между этапами производственного процесса, поддерживают разные версии и стадии разработки (согласование, утверждение и т.д.) документов. Это способствует снижению себестоимости и времени выполнения работ, росту производительности труда.

Процедуры, регламентирующие все производственные операции, также представляют собой электронные документы и хранятся в архиве. После создания они проходят следующие стадии жизненного цикла: маршрутизация для просмотра и комментирования, редактирование, окончательное утверждение и определение срока действия, уведомление пользователей, введение процедуры в действие. В течение всего срока действия процедуры необходимо вести контроль вносимых в нее изменений. Управление операционными процедурами ведется ПО архива. При этом ускоряется процесс разработки, просмотра и утверждения процедур, обеспечивается

непрерывный доступ пользователей, контроль сроков выполнения. Каждое действие при работе с архивом должно фиксироваться с целью последующего анализа и создания отчетов. Информация о запросах к хранимым документам помогает отслеживать нарушения информационной безопасности.

Процедуры затрагивают и вопросы разработки новых технических документов, в частности с использованием разработанных ранее и уже размещенных в архиве [6]. При этом приходится работать с большим объемом неструктурированных данных, подготовленных в различных средах. Эффективность форматирования и объединения информации повышается с помощью средств создания виртуальных документов – редакторов XML, например XMetal.

Другой метод взаимодействия участников проекта – Web-технологии. Например, коллективная работа может быть основана на концепции виртуальных комнат (eRoom) [7]. Проектная среда представляет собой защищенное рабочее пространство, основанное на интерфейсе браузера, и легко адаптируется в соответствии с требованиями каждого проекта. Через eRoom исполнители имеют общий доступ к хранилищу данных проекта и работают, как если бы они находились территориально в одном месте.

Все перечисленные средства информационной поддержки являются инвариантными по отношению к назначению и структуре системы. Существуют и другие обязательные компоненты хранилища, зависящие от конкретной задачи. Речь идет о программных средствах взаимодействия с функциональными системами разработки изделий: инструментальными комплексами систем проектирования; системами автоматизации производства, инженерного анализа, взаимодействий с заказчиком и т.д.

ПРОБЛЕМА МИГРАЦИИ ДАННЫХ ИЗ СУЩЕСТВУЮЩИХ ХРАНИЛИЩ ДОКУМЕНТАЦИИ В ПЕРСПЕКТИВНЫЕ

Одной из фундаментальных отличительных черт больших систем является эволюционный характер их развития. Разработка документации ведется на протяжении многих лет с использованием самых разных инструментальных средств. Поэтому при внедрении новых технологий хранения встает проблема переноса (миграции) информации из одной среды в другую. Задача усложняется из-за разнородности данных и платформ, на которых они были созданы. Для корректной миграции сначала следует исследовать совместимость СУБД, работающих с хранилищами электронных документов старой и новой систем. Основные отличия касаются логической и физической организации хранения данных (распределение таблиц, индексов и других объектов базы по файлам, владельцам и т.п.), структуры баз данных (типы данных и размеры полей, ограничения на поля, индексы, первичные и внешние ключи, ссылки между таблицами и т.п.), программирования процедур и пользовательских функций, запросов, команд и операторов (конструкции запросов, встроенные функции и т.п.), методов преобразования данных (обработка пустых полей, конвертирование дат в числа или строк в числа и т.п.), распределения прав доступа. Также нужно обратить внимание на методы администрирования и сопровождения серверов, поддержку различных операционных систем, протоколов взаимодействия клиента с сервером и протоколов транспортного уровня (TCP/IP/, IPX/SPX, NetBIOS).

В большинстве случаев для переноса данных применяют средства инженерного анализа и моделирования (Computer Aided Software/System Engineering, CASE-средства), например ERWin или Power Designer. Иногда – встроенные в СУБД средства экспорта данных из базы в отдельный файл. Кроме того, разрабатывают специализированные программы-конверторы верхнего уровня (ADO, OLEDB, ODBC и т.д.). Каждый из перечисленных подходов имеет свои преимущества и недостатки, определяемые конкретной задачей, тем более что речь идет о разовом применении. На практике для миграции достаточно сложных БД реализуются различные комбинации перечисленных методов, что увеличивает трудоемкость и временные затраты. Впрочем, вне зависимости от подхода, процесс миграции сводится к типовой процедуре. Сначала проводится анализ форматов данных и струк-

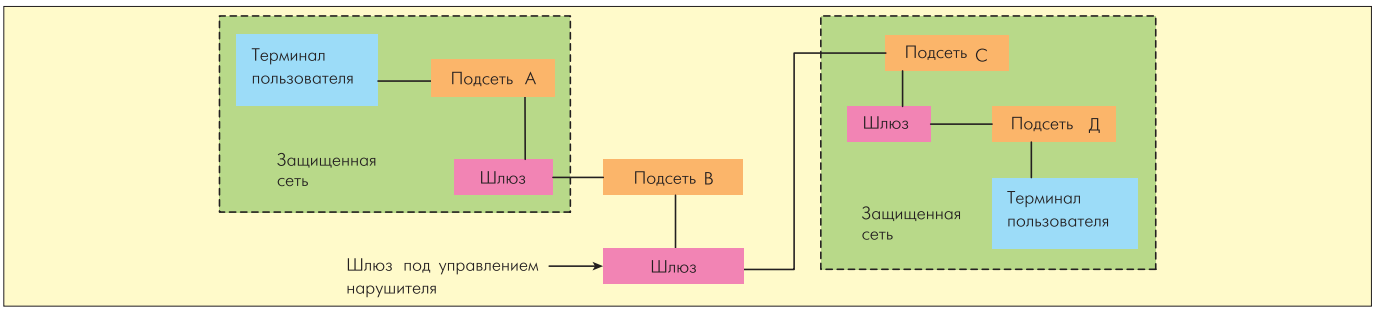

Рис.4. Схема подключения нарушителя к локальной вычислительной сети. Нарушитель контролирует шлюз на единственном пути между двумя интересующими его процессами. Подсети источника (А) и адресата (Д) защищены, но соединение, проходящее через подсети В и С, уязвимо для атак

туры старой и новой БД, определение взаимосвязей между таблицами (иерархии объектов). Далее принимается решение о последовательности закачки данных в соответствии с иерархией зависимостей, выполняется скрипт по изменению объектов в новой версии БД. После этого происходит непосредственно перекачка данных, их преобразование и восстановление отключенных индексов.

Перспективной видится разработка инструментальных средств миграции с использованием универсального преобразователя языков. Принцип работы такого конвертера основан на технологии толерантной трансляции [8], то есть выделении похожих элементов в тексте, не связанных с конкретным языком. Замена этих элементов производится на основе синтаксических правил и структур, которые может составлять сам пользователь с помощью языка программирования верхнего уровня.

РАЗГРАНИЧЕНИЕ ДОСТУПА И ЗАЩИТА ЭЛЕКТРОННЫХ АРХИВНЫХ ДАННЫХ

Поскольку корпоративные хранилища содержат практически всю документацию по функционированию целой структуры, отсутствие защиты данных связано с серьезными финансовыми потерями. Речь идет о нарушении коммерческой или государственной тайны, авторских прав. Пример недостаточно действенных мер – появление в свободной продаже баз данных ГИБДД, кредитных историй банков и др. Отсутствие надежных средств защиты информации, в том числе от инсайдеров, привело к нарушению Федерального закона "О персональных данных" в массовом масштабе.

Воздействие на информацию – это реализация случайных или преднамеренных угроз. Причинами случайного воздействия могут стать: отказ технических средств; алгоритмические и программные ошибки; некорректные действия эксплуатационного персонала; стихийные бедствия; нарушение функционирования объекта, на котором размещено хранилище. Могут навредить и помехи на линиях связи, вызванные дестабилизирующими факторами внешней среды, например расположением технических средств хранилища относительно друг друга и других систем.

Преднамеренные угрозы связаны с целенаправленными действиями человека-злоумышленника. При отсутствии защиты он может использовать в своих интересах штатные каналы передачи данных; электромагнитное излучение технических средств архива; наводки по сети электропитания на вспомогательных коммуникациях; отходы обработки информации и т.д. При организации хранилища на локальной вычислительной сети есть угроза подключения нарушителя к коммуникациям (рис.4).

Серьезную опасность представляет собой бесконтрольная загрузка ПО, так как при этом могут быть изменены данные, или введена программа типа "троянский конь", предназначенная для записи информации на посторонний носитель или передачи во внешние каналы связи.

Основной метод защиты от преднамеренного несанкционированного доступа – функциональный контроль и диагностика отказов и сбоев аппаратуры, программных ошибок. Также к обязательным мерам относятся: контроль доступа к внутреннему монтажу и управлению техническими средствами хранилища, а также к линиям связи; защита от излучения и наводок; аутентификация пользователей, технических средств хранилища и носителей данных.

Необходимыми условиями функционирования электронных архивов большой емкости, являются разграничение доступа и защита информации. Несанкционированный доступ приводит к утрате конфиденциальности информации, ее исчезновению или замене на ложную. Поэтому данные следует разделить на сегменты и организовать доступ к ним в соответствии с обязанностями и полномочиями пользователей. Деление должно производиться по степени важности, функциональному назначению и конкретным перечням документов. Поскольку

доступ к информации осуществляется с различных технических средств хранилища, необходимо разграничить доступ с целью проведения регламентных работ и загрузки ПО от выполнения обработки информации. Целесообразно, чтобы обслуживание и ремонт технических средств выполнял персонал, не имеющий доступа к защищенной информации, а любые изменения ПО производили специально выделенные сотрудники. Также следует разделить процессы регистрации оперативной и технологической информации.

Доступ пользователей к хранилищу необходимо регулировать в зависимости от вида, назначения и степени важности информации, способа обработки данных и т.д. Информацию можно разделить на четыре класса [9]:

- жизненно важная, модификация которой приведет к невосполнимым потерям;
- важная, доступная небольшой группе пользователей;
- информация, постоянный несанкционированный доступ к которой может привести к утечке более ценных данных;
- не представляющая конкретного интереса для злоумышленников, но требующая защиты от случайных нарушений из-за безответственности исполнителей.

Наиболее часто на практике применяют системы защиты в виде трех составных частей: основного контура безопасности, средств противодействия случайному несанкционированному доступу и средств управления системой защиты. Основной контур выполняет функции защиты носителей данных (как съемных, так и несъемных), защиты технических средств от несанкционированного вскрытия, контроля вывода аппаратуры из рабочего режима в режим выполнения регламентных работ. Для защиты носителей данных достаточно специального ПО шифрования данных, уничтожения остатков информации с носителей и аутентификации информации на носителях (использование инфраструктуры открытых ключей, и т.д.). Контроль технических средств лучше вести аппаратно, с применением разнородных датчиков с электронным выходом. Предотвратить случайный несанкционированный доступ позволяют специальные программные решения: кодирование каналов связи с помощью ЕСС; введение контрольных точек в приложения обработки данных; проверка целостности информации путем контрольного суммирования и др. Центральный элемент системы информационной безопасности – автоматизированное рабочее место службы безопасности. На нем ведется журнал учета и сбор статистики по работе пользователей, контроль аппаратуры записи паролей, управление программами шифрования данных и т.д.

Предложенные методы – не единственный путь решения сложной задачи создания и модернизации больших электронных хранилищ документации. Тем более, что в процессе их построения нужно учитывать особенности конкретного промышленного объединения и сложность разрабатываемых и производимых им изделий. Однако есть надежда, что обсуждение этой актуальной проблемы будет содействовать выработке оптимальных путей ее решения.

ОБ АВТОРЕ

Журавский Виталий Григорьевич – доктор технических наук, профессор, действительный член Российской академии естественных наук, заслуженный деятель науки РФ, заслуженный машиностроитель РФ, лауреат Государственной премии СССР и Премии Правительства РФ. Удостоен отечественных и зарубежных наград. Сфера научных интересов – конструкторско-технологическое обеспечение больших АСУ. Обладатель 50 патентов на объекты интеллектуальной деятельности. Автор более 150 опубликованных научных работ, в том числе пяти монографий.

ЛИТЕРАТУРА

1. **Гольдин В.В.** Электронная цифровая подпись технической документации. – Проектирование и технология электронных средств, 2003, № 3.
2. ГОСТ 2.051-2006 ЕСКД. Электронные документы. Общие положения.
3. **Гольдин В.В., Журавский В.Г., Сарафанов А.В., Кофанов Ю.Н.** Информационная поддержка жизненного цикла электронных средств. – М.: Радио и связь, 2002.
4. **Чеботарев А.Н.** Развитие интеллекта систем хранения данных.// Сети и телекоммуникации, 2006, № 2.
5. **Залещанский Б.Д., Чернихов Д.Я.** Кластерная технология и живучесть глобальных автоматизированных систем. – М: Финансы и статистика, 2005.
6. **Журавский В.Г., Гольдин В.В., Чашков Ю.А.** Опыт внедрения компонентов CALS-технологий при создании технических средств АСУ. – Информационные технологии в проектировании и производстве, 2003, № 4.
7. **Яцкевич А.И., Дещеревский И.В.** Технология представления информации об изделии. Система управления конструкторскими данными о машиностроительном изделии. – Информационные технологии в проектировании и производстве, 2000, № 2.
8. **Гольдин В.В., Журавский В.Г., Правильщиков П.А.** Применение методов толерантной трансляции для разработки универсальных конверторов данных. – В кн.: Материалы 5 Международной конференции CAD/CAM/PDM-2005 – М.: ИПУ, 2005.
9. **Мельников В.В.** Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ. 1997. 2005.
10. **Пятибратов А.П., Гудыно Л.П., Кириченко А.А.** Вычислительные системы, сети и телекоммуникации. – М: Финансы и статистика, 2004.
11. **Мельников Д.А.** Информационные процессы в компьютерных сетях. – М.: Кудиц-образ, 2001.
12. **Журавский В.Г., Гольдин В.В., Котов А.Г., Уробушкин В.И.** Методы и средства разработки и функционирования системы электронного документооборота на предприятии=разработчике. – Качество и ИПИ (CALS)-технологии, 2006, № 4.
13. **Журавский В.Г., Гольдин В.В.** Опыт информационной поддержки создания комплексов технических средств АСУ. – Качество и ИПИ (CALS)-технологии, 2005, № 4.