Защита информационных и физических объектов ИС

В этой главе

- *Файлы и базы данных как информационные объекты защиты*
- *Защита ресурсных объектов*
- *Защита физических объектов ИС*
- *Охранное видеонаблюдение*

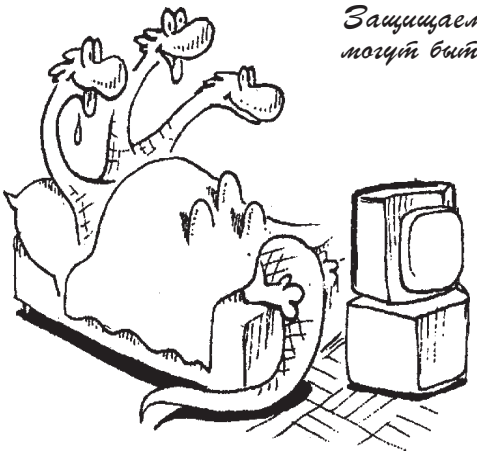
<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Файлы и базы данных как информационные объекты защиты (010)

Защищаемые файлы (013)

Рассмотрим вопросы обеспечения сохранности накапливаемой информации в отдельных файлах и базах данных.

Часто файлы размещаются на различных носителях информации и принадлежат пользователям ИС. Их коллективное использование определяет необходимость в организации защиты отдельных файлов от несанкционированного использования, а также от физического разрушения. Проблема усложняется и в связи с тем, что пользователи могут предоставлять свои файлы другим пользователям. Таким образом, все защищаемые файлы можно условно классифицировать как: общие, групповые, личные.



Для обеспечения сохранности файлов могут быть использованы аппаратные и программные средства защиты, а также совокупность мероприятий организационного плана, позволяющих проводить учет, хранение и использование файлов.

Распределенное хранение файлов

Проблемы

Файловые серверы могут контролировать доступ пользователей к различным частям файловой системы путем разрешения пользователю присоединить некоторую файловую систему (или каталог) к своей рабочей станции для использования как локального диска. Это порождает две потенциальные проблемы.

Первая состоит в том, что сервер может обеспечить защиту доступа только на уровне каталога, поэтому если пользователю разрешен доступ к каталогу, то он получает доступ ко всем файлам, содержащимся в этом каталоге. Чтобы минимизировать риск в этой ситуации, важно соответствующим образом структурировать и управлять файловой системой ЛВС.

Вторая проблема заключается в неадекватных механизмах защиты локальной рабочей станции. Например, персональный компьютер (ПК) может обеспечивать минимальную защиту или не обеспечивать никакой защиты информации, хранимой на нем.

Копирование пользователем файлов с сервера на локальный диск ПК приводит к тому, что файл перестает быть защищенным теми средствами защиты, которые защищали его, когда он хранился на сервере. Для некоторых типов информации это может быть приемлемо. Однако, другие типы информации могут требовать более сильной защиты. Эти требования приводят к необходимости контроля среды ПК.

Защита баз данных (013)

Системы управления базами данных, в особенности реляционные СУБД, стали доминирующим инструментом хранения больших массивов информации. Сколько-нибудь развитые информационные приложения полагаются не на файловые структуры операционных систем, а на многопользовательские СУБД, выполненные в технологии клиент/сервер. В этой связи обеспечение информационной безопасности СУБД, и в первую очередь их серверных компонентов, приобретает решающее значение для безопасности организации в целом.

Для СУБД важны все три основных аспекта информационной безопасности — конфиденциальность, целостность и доступность. Общая идея защиты баз данных состоит в следовании рекомендациям, сформулированным в "Критериях оценки надежных компьютерных систем".

Организация хранения и использования информации в базах данных (БД) имеет специфические особенности. Если к информации, содержащейся в БД, обращаются многие пользователи, то особенно важно, чтобы элементы данных и связи между ними не разрушались. Следует также учитывать возможность возникновения ошибок и различного рода случайных сбоев. Хранение, обновление и процедуры включения данных должны быть такими, чтобы система в случае возникновения сбоев могла восстанавливать данные без потерь.

Степень сохранности информации в БД повышается, если она защищена от аппаратных и программных сбоев, катастрофических и криминальных ситуаций, некомпетентности или злоумышленного использования.

Когда рассматриваются процедуры защиты сетевых баз данных, то данные и их логические структуры представляются двумя способами. Отдельные объекты данных сами могут быть объектами защиты, но могут быть организованы в структуры БД (сегменты, отношения, каталоги и т.п.).

Защита БД означает защиту собственно данных и их контролируемое использование на рабочих местах сети, а также защиту любой сопутствующей информации, извлекаемой или генерируемой из этих данных.

Это важно

Функции, процедуры и средства защиты, обеспечивающие защиту данных на рабочих станциях сети, можно описать следующим образом:

1. *Защита содержания данных* объединяет функции, процедуры и средства защиты, которые предупреждают несанкционированное раскрытие конфиденциальных данных и информации из БД.

2. *Средства контроля доступа* разрешают доступ к данным только полномочных объектов в соответствии со строго определенными правилами и условиями.

3. *Управление потоком защищенных данных* при передаче из одного сегмента БД в другой обеспечивает перемещение данных вместе с механизмами защиты, присущими исходным данным.

4. *Предотвращение возможности выявления* конфиденциальных значений из данных, содержащихся в регулярных или схоластических БД, в результате выявления статистически достоверной информации.

5. *Контроль согласованности* при использовании БД предполагает процедуры защиты, которые обеспечивают защиту и целостность отдельных элементов данных. Успешная реализация таких процедур в ИС означает, что данные в БД всегда логически связаны и значения критических данных передаются от узла к узлу только при наличии специальных полномочий

6. *Контекстная защита данных*, характерная для схем защиты динамических БД, также должна быть включена в состав процедур защиты БД. В этом случае защита отдельного элемента БД в каждый момент времени зависит от проведения всей системы защиты, а также предшествующих операций, выполненных над этим элементом (зависимость от предыстории).

7. *Предотвращение создания несанкционированной информации* предполагает наличие средств, которые предупреждают, что объект получает (генерирует) информацию, превышающую уровень прав доступа, и осуществляет это, используя логическую связь между данными в БД.

Надо знать

Известны два способа защиты данных в сетевых базах. Первый, наиболее очевидный, заключается в запрещении доступа к данным пользователям сети, не имеющим права доступа к ним. Управление доступом позволяет регулировать просмотр, изменение и удаление данных и программ. Подобное управление предотвращает случайное или преднамеренное обнаружение, изменение или уничтожение записей и наборов данных.

Второй, также эффективный способ защиты баз данных в ИС состоит в обеспечении гарантийного доступа ко всем необходимым данным тем пользователям сети, которые правильно используют возможности и свои права.

Эффективность механизма управления доступом для защиты данных в ИС зависит от выполнения трех предположений.

1. **Правильная идентификация пользователя** с целью запретить использование СУБД на основе прав другого пользователя. Схемы идентификации используют пароли как наиболее распространенный способ достижения этой цели.

2. **Злоумышленники не должны иметь доступа к разделам базы данных**, если даже они выкрали магнитные ленты или пакеты дисков или прослушали линий связи. Обычно в качестве механизма защиты для решения этой проблемы используется шифрование.

При получении шифрованных данных пользователь должен их расшифровать, затем выполнить необходимые действия и, наконец, снова зашифровать. Кроме того, в распределенных сетевых базах данных на разных рабочих станциях можно применять различные алгоритмы шифрования и криптографические ключи.

3. **Информацию о правах доступа субъектов необходимо тщательно охранять**: подразумевается информация, определяющая доступ каждой программы к объектам системы. Категории секретности можно использовать в базах данных в том случае, если СУБД — отправитель, а пользователь — получатель. Пользователь может получить доступ к данным и тогда, когда он имеет такую же или более высокую категорию секретности, чем данные. В этом случае база данных (или ее части) должна иметь некоторый набор атрибутов для указания категории секретности.

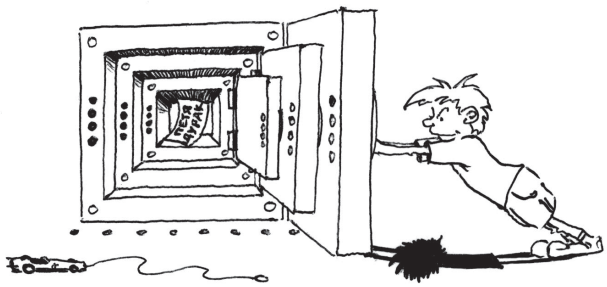
Средства управления данными в СУБД разрешают пользователю управлять доступом других пользователей к его данным и контролировать неприкосновенность последних. Средства защиты могут также обеспечивать выполнение групповых операций (транзакций) и осуществлять восстановление БД.

В большинстве сетевых СУБД установлена ответственность каждого пользователя за управление доступом к созданному им объекту. Когда пользователь создает некий объект (представление данных) и определяет операции отношения, то он должен в полном объеме контролировать выполняемые действия. (Если задано представление, то права доступа к нему обычно ограничены уже имеющимися полномочиями на выполнение определенных операций). Пользователь может предоставить право доступа к объектам и операциям другому пользователю.

В большинстве сетевых механизмов управления доступом допускаются такие атрибуты:

READ — чтение
INSERT — вставка
DELETE — удаление
UPDATE — обновление
EXPAND — расширение
IMAGE — создание образа
CONTROL — управление

Вместе с тем пользователь может передать кому-либо права установки атрибутов доступа. Однако это может сделать только пользователь, имеющий соответствующий атрибут доступа.



Нужны надежные механизмы защиты данных...

Атрибут доступа может быть как установлен, так и снят (отменен). Он удаляется из списка атрибутов того пользователя, который его установил, и всех пользователей, которым данный атрибут был передан этим пользователем, исключая тех, кому удаляемый атрибут был установлен другим пользователем. Процесс отмены атрибута может также иметь и другие особенности.

Для упрощения поддержки целостности базы данных пользователь может определить в некоторой отдельной таблице переключатель, используемый при выполнении операций (READ, INSERT, DELETE, UPDATE). Переключатель, содержащий один или несколько операторов управления, выполняется непосредственно после описанных действий пользователя. Если оператор предназначен для выполнения операций обновления над несколькими элементами, это реализуется поэлементно. Переключатели всегда выполняются немедленно и не могут быть отложены до окончания операции. В теле переключателя могут использоваться опции OLD и NEW, указывающие на прежние и обновленные величины.

Если информация, получаемая на основе конфиденциальных данных, предназначена для широкого использования, то требуют изменений правила управления потоком передаваемых данных. Это относится в первую очередь к статистическим базам и банкам данных, которые содержат конфиденциальную информацию о личности, используемую для формирования различных статистических сводок.

Особенность ситуации состоит в том, что сводки содержат “отголоски” исходной конфиденциальной информации, и весьма настойчивый пользователь может ее восстановить. Когда информация касается некоторого конкретной личности, процедура восстановления расценивается как посягательство на его личную тайну.

Определение

Запись считается скомпрометированной, если пользователь, формирующий запрос, может определить значение конфиденциальной величины, сравнивая ответы на запросы и используя любую априорную информацию. Компрометация состоит в выявлении интересующей записи на основе перекрестных запросов; искажении ответа путем округления или некоторой преднамеренной коррекции данных; контроль обращения только к случайным записям.

Доступ к информации на основе *метода выслеживания* основан на использовании группы пересекающихся записей. Для защиты от выслеживания применяют принцип минимальной взаимосвязи вопросов, который состоит в следующем: “Не следует отвечать на запрос, в котором содержится более определенного числа совпадающих записей из предыдущих запросов”.

Такой контроль на практике нереален, поскольку программа должна произвести сравнение последней группы запросов со всеми предыдущими. Но если даже к нему и прибегнуть, этот контроль можно обойти в базе данных, где каждая конфиденциальная величина появляется лишь один раз. Контроль минимальной взаимосвязи вопросов может быть устранен путем решения системы линейных уравнений относительно неизвестной величины.

Другой способ контроля за логическим выводом основан на *внесении преднамеренных искажений* в ответы. Обычно реализуется округление результатов, ког-

да точный ответ на запрос незначительно искажается, прежде чем сформируется ответ пользователю на его запрос.

Еще один способ контроля основан на том, что ***запросы адресуются не ко всей базе данных***, а к некоторой случайно выбранной группе записей. Такой подход наиболее эффективен, поскольку лишает пользователя возможности контролировать множество запросов. Функции запросов в большинстве коммерческих СУБД позволяют выявить значительно больше информации о конфиденциальных записях, чем представляется. Без соответствующего контроля несанкционированный доступ к базе данных будет скорее правилом, чем исключением. В комбинации с принципом минимального множества запросов случайные запросы обеспечивают наилучшую защиту.

Наиболее эффективной мерой защиты от навязчивых злоумышленников является наблюдение за вторжениями, включающее проверку файлов регистрации и контрольных журналов на наличие необычных сочетаний запросов или большого числа запросов к одной и той же записи. Хотя при этом и контролируется поток информации, проходящей через программы обработки запросов, но наблюдение за вторжениями позволяет выявить повышенную активность обращений.

Идентификация и проверка подлинности пользователей (710)

Обычно в СУБД для идентификации и проверки подлинности пользователей применяются либо соответствующие механизмы операционной системы, либо SQL-оператор CONNECT.

Так или иначе, в момент начала сеанса работы с сервером баз данных, пользователь идентифицируется своим именем, а средством аутентификации служит пароль. Детали этого процесса определяются реализацией клиентской части приложения.

Некоторые операционные системы, такие как UNIX, позволяют во время запуска программы менять действующий идентификатор пользователя. Приложение, работающее с базой данных, как правило, имеет привилегии, значительно превосходящие привилегии обычных пользователей. Естественно, что при этом приложение предоставляет тщательно продуманный, строго фиксированный набор возможностей. Если пользователь сумеет тем или иным способом завершить приложение, но сохранить подключение к серверу баз данных, ему станут доступны по существу любые действия с данными.

Угрозы для СУБД

Главный источник угроз, специфичных для СУБД, лежит в самой природе баз данных. Основным средством взаимодействия с СУБД является язык SQL - мощный непроцедурный инструмент определения и манипулирования данными. Хранимые процедуры добавляют к этому репертуару управляющие конструкции. Механизм правил дает возможность выстраивать сложные, трудные для анализа цепочки действий, позволяя попутно неявным образом передавать право на выполнение процедур, даже не имея, строго говоря, полномочий на это. В результате потенциальный злоумышленник получает в свои руки мощный и удобный инструментарий, а все развитие СУБД направлено на то, чтобы сделать этот инструментарий еще мощнее и удобнее.

Получение информации путем логических выводов

Нередко путем логического вывода можно извлечь из базы данных информацию, на получение которой стандартными средствами у пользователя не хватает привилегий. Если для реализации контроля доступа используются представления, и эти представления допускают модификацию, с помощью операций модификации/вставки можно получить информацию о содержимом базовых таблиц, не располагая прямым доступом к ним.

Основным средством борьбы с подобными угрозами, помимо тщательно проектирования модели данных, является механизм размножения строк. Суть его в том, что в состав первичного ключа, явно или неявно, включается метка безопасности, за счет чего появляется возможность хранить в таблице несколько экземпляров строк с одинаковыми значениями "содержательных" ключевых полей.

Борьба с получением информации путем логического вывода требует кропотливого труда при проектировании модели данных и иерархии привилегий, а также при реализации видимых пользователям представлений.

Агрегирование данных (220)

Агрегирование — это метод получения новой информации путем комбинирования данных, добытых легальным образом из различных таблиц. Агрегированная информация может оказаться более секретной, чем каждый из компонентов, ее составивший. В качестве примера можно рассмотреть базу данных, хранящую параметры всех комплектующих, из которых будет собираться ракета, и инструкцию по сборке.

Повышение уровня секретности данных при агрегировании вполне естественно — это следствие закона

перехода количества в качество. Бороться с агрегированием можно за счет тщательного проектирования модели данных и максимального ограничения доступа пользователей к информации.

Управление доступом (750)

Основные понятия (751)

Обычно в СУБД применяется произвольное управление доступом, когда владелец объекта передает права доступа к нему (чаще говорят — привилегии) по своему усмотрению. Привилегии могут передаваться субъектам (отдельным пользователям), группам, ролям или всем пользователям.

Группа — это именованная совокупность пользователей. Объединение субъектов в группы облегчает администрирование баз данных и, как правило, строится на основе формальной или фактической структуры организации. Каждый пользователь может входить в несколько групп. Когда пользователь тем или иным способом инициирует сеанс работы с базой данных, он может указать, от имени какой из своих групп он выступает. Кроме того, для пользователя обычно определяют подразумеваемую группу.

Роль — это еще один возможный именованный носитель привилегий. С ролью не ассоциируют перечень допустимых пользователей — вместо этого роли защищают паролями. В момент начала сеанса с базой данных можно специфицировать используемую роль (обычно с помощью флагов или эквивалентного механизма) и ее пароль, если таковой имеется.

Привилегии роли имеют приоритет над привилегиями пользователей и групп. Иными словами, пользователю как субъекту не обязательно иметь права доступа к объектам, обрабатываемым приложениям с определенной ролью.

В СУБД Oracle под ролью понимается набор привилегий. Такие роли служат средством структуризации привилегий и облегчают их модификацию.

Основные категории пользователей (752)

Пользователей СУБД можно разбить на три категории:

- администратор сервера баз данных. Он ведает установкой, конфигурированием сервера, регистрацией пользователей, групп, ролей и т.п. Администратор сервера имеет имя ingres. Прямо или косвенно он обладает всеми привилегиями, которые имеют или могут иметь другие пользователи.
- администраторы базы данных. К этой категории относится любой пользователь, создавший базу данных, и, следовательно, являющийся ее владельцем. Он может предоставлять другим пользователям доступ к базе и к содержащимся в ней объектам. Администратор базы отвечает за ее сохранение и восстановление. В принципе в организации может быть много администраторов баз данных. Чтобы пользователь мог создать базу и стать ее администратором, он должен получить (вероятно, от администратора сервера) привилегию creatdb.
- ***Прочие*** (конечные) пользователи. Они оперируют данными, хранящимися в базах, в рамках выделенных им привилегий.

Администратор сервера баз данных, как самый привилегированный пользователь, нуждается в особой защите. Компрометация его пароля фактически означает компрометацию сервера и всех хранящихся на нем баз данных.

Поручать администрирование различных баз данных разным людям имеет смысл только тогда, когда эти базы независимы и по отношению к ним не придется проводить согласованную политику выделения привилегий или резервного копирования. В таком случае каждый из администраторов будет знать ровно столько, сколько необходимо.

Введение служебных пользователей позволяет администрировать функциональные подсистемы, не получая привилегий суперпользователя. Точно так же информацию, хранящуюся на сервере баз данных, можно разделить на отсеки, так что компрометация администратора одного отсека не означает обязательной компрометации другого.

Виды привилегий

Привилегии в СУБД можно подразделить на две категории: привилегии безопасности и привилегии доступа. ***Привилегии безопасности*** позволяют выполнять административные действия. ***Привилегии доступа***, в соответствии с названием, определяют права доступа субъектов к определенным объектам.

Привилегии безопасности

Привилегии безопасности всегда выделяются конкретному пользователю.

Таких привилегий пять:

- ***security*** — право управлять безопасностью СУБД и отслеживать действия пользователей. Пользователь с этой привилегией может подключаться к любой базе данных, создавать, удалять и изменять характеристики пользователей, групп и ролей, передавать права на доступ к базам данным другим пользователям, управлять записью регистрационной информации, отслеживать запросы других пользователей и, наконец, запускать INGRES-команды от имени других пользователей. Привилегия security необходима администратору сервера баз данных, а также лицу, персонально отвечаю-

щему за информационную безопасность. Передача этой привилегии другим пользователям (например, администраторам баз данных) увеличивает число потенциально слабых мест в защите сервера баз данных.

- ***createdb*** — право на создание и удаление баз данных. Этой привилегией, помимо администратора сервера, должны обладать пользователи, которым отводится роль администраторов отдельных баз данных.
- ***operator*** — право на выполнение действий, которые традиционно относят к компетенции оператора. Имеются в виду запуск и остановка сервера, сохранение и восстановление информации. Помимо администраторов сервера и баз данных этой привилегией целесообразно наделить также администратора операционной системы.
- ***maintain_locations*** — право на управление расположением баз администраторы сервера баз данных и операционной системы.
- ***trace*** — право на изменение состояния флагов отладочной трассировки. Данная привилегия полезна администратору сервера баз данных и другим знающим пользователям при анализе сложных, непонятных ситуаций.

Привилегии доступа (750)

Привилегии доступа выделяются отдельным пользователям, группам, ролям или всем пользователям. Эти привилегии, как правило, присваивает владелец соответствующих объектов (он же — администратор базы данных) или обладатель привилегии security (обычно администратор сервера баз данных). При совершении подобных действий необходимо иметь подключение к базе данных, в которой хранятся сведения о субъектах и их привилегиях.

Привилегии доступа можно подразделить в соответствии с видами объектов, к которым они относятся:

- таблицы и представления
- процедуры
- базы данных
- сервер баз данных
- события

По умолчанию пользователь не имеет никаких прав доступа к таблицам и представлениям.

По отношению к процедуре можно предоставить право на выполнение. При этом не нужно заботиться о выделении прав доступа к объектам, обрабатываемым процедурой — их наличие не обязательно. Таким образом, процедуры баз данных являются удобным средством предоставления контролируемого доступа для выполнения строго определенных действий над данными.

При создании базы данных указывается ее статус - общая или личная. Это влияет на подразумеваемые права доступа к базе. По умолчанию право на подключение к общей базе предоставляется всем. Право на подключение к личной базе нужно передавать явным образом. Право на подключение необходимо для выполнения всех прочих операций с базой и содержащимися в ней объектами.

По умолчанию все пользователи имеют право создавать процедуры в базах данных. Если бы они при этом автоматически получали права на выполнение, то смогли бы осуществить по существу любую операцию с данными, поскольку выполнение процедуры не требует прав доступа к обрабатываемым объектам. К счастью, для передачи привилегии доступа к объектам, и в, частности, для предоставления права на выполнение процедуры, надо быть не только владельцем объекта, но и администратором базы данных. Мы видим, насколько осторожно нужно относиться к предоставлению привилегий выполнения по отношению к новым, непроверенным процедурам. В принципе достаточно одного "троянского коня", чтобы скомпрометировать всю базу данных. Процедуры являются столь же гибким, но и столь же опасным средством, что и UNIX-программы с битом переустановки действующего идентификатора пользователя.

Метки безопасности и принудительный контроль доступа (750)

Средства произвольного управления доступом не могут помешать авторизованному пользователю законным образом получить секретную информацию и затем сделать ее доступной для других, неавторизованных пользователей. При произвольном управлении доступом привилегии существуют отдельно от данных (в случае реляционных СУБД — отдельно от строк реляционных таблиц). В результате данные оказываются "обезличенными", и ничто не мешает передать их кому угодно даже средствами самой СУБД.

В "Критериях оценки надежных компьютерных систем" описан механизм меток безопасности. Применять его на практике имеет смысл только в сочетании с операционной системой и другими программными компонентами того же уровня безопасности. Метка безопасности состоит из трех компонентов:

- ***Уровень секретности.*** Смысл этого компонента зависит от приложения. В частности, возможен традиционный спектр уровней от "совершенно секретно" до "несекретно".
- ***Категории***. Понятие категории позволяет разделить данные на "отсеки" и тем самым повысить надежность системы безопасности. В коммерческих приложениях

категориями могут служить "финансы", "кадры", "материальные ценности" и т.п. Ниже назначение категорий разъясняется более подробно.

- ***Области***. Является дополнительным средством деления информации на отсеки. На практике компонент "область" может действительно иметь географический смысл, обозначая, например, страну, к которой относятся данные.

Каждый пользователь СУБД характеризуется степенью благонадежности, которая также определяется меткой безопасности, присвоенной данному пользователю. Пользователь может получить доступ к данным, если степень его благонадежности удовлетворяет требованиям соответствующей метки безопасности. А именно:

- уровень секретности пользователя должен быть не ниже уровня секретности данных;
- набор категорий, заданных в метке безопасности данных, должен целиком содержаться в метке безопасности пользователя;
- набор областей, заданных в метке безопасности пользователя, должен целиком содержаться в метке безопасности данных.

Механизм меток безопасности не отменяет, а дополняет произвольное управление доступом. При добавлении или изменении строк пользователи, как правило, наследуют метки безопасности. Таким образом, даже если авторизованный пользователь перепишет секретную информацию в общедоступную таблицу, менее благонадежные пользователи не смогут ее прочитать.

Поддержание целостности данных в СУБД (724)

Для коммерческих организаций обеспечение целостности данных не менее важно, чем обеспечение конфиденциальности. Конечно, неприятно, когда кто-то подглядывает за суммами на счетах клиентов, но гораздо хуже, когда в процессе перевода денег со счета на счет часть суммы исчезает в неизвестном направлении.

Известно, что главными врагами баз данных являются не внешние злоумышленники, а ошибки оборудования, администраторов, прикладных программ и пользователей. С точки зрения пользователя СУБД, основными средствами поддержания целостности данных являются ограничения и правила.

Ограничения могут относиться к таблицам или отдельным столбцам. При массовом копировании данных контроль ограничений отключается. Это значит, что необходимо дополнять копирование запуском процедуры глобальной проверки целостности.

Правила позволяют вызывать выполнение заданных действий при определенных изменениях базы данных. Обычно действие — это вызов процедуры. Правила ассоциируются с таблицами и срабатывают при изменении этих таблиц.

В отличие от ограничений, которые являются лишь средством контроля относительно простых условий, правила позволяют проверять и поддерживать сколь угодно сложные соотношения между элементами данных в базе.

Как и в случае ограничений, проверка правил отключается при массовых операциях копирования. Администратор базы данных может также явным образом отменить проверку правил.

Пользователь, действия которого вызывают срабатывание правила, должен обладать лишь необходимыми правами доступа к таблице. Тем самым правила неявно расширяют привилегии пользователей. Подобные расширения нуждаются в строгом административном контроле, поскольку даже незначительное изменение правила или ассоциированной процедуры может кардинально повлиять на защищенность данных. Ошибка же в сложной системе правил вообще чревата непредсказуемыми последствиями.

Средства поддержания высокой готовности (724)

В коммерческих приложениях высокая готовность аппаратно-программных комплексов является важнейшим фактором. Применительно к СУБД средства поддержания высокой готовности должны обеспечивать нейтрализацию аппаратных отказов, особенно касающихся дисков, а также восстановление после ошибок обслуживающего персонала или прикладных программ.

Подобные средства должны с самого начала закладываться в архитектуру комплекса. Например, необходимо использовать тот или иной вид избыточных дисковых массивов. Конечно, это сделает аппаратно-программное решение более дорогим, но зато убережет от возможных убытков во время эксплуатации.

Кластерная организация сервера баз данных (724)

Под кластером будем понимать конфигурацию из нескольких компьютеров (узлов), выполняющих общее приложение (такое, например, как сервер баз данных). Обычно кластер содержит также несколько дисковых подсистем, совместно используемых узлами-компьютерами, и избыточные связи между компонентами. С внешней точки зрения кластер выглядит как единое целое, а наличие нескольких узлов способствует повышению производительности и устойчивости к отказам.

Подобная аппаратная архитектура обеспечивает устойчивость к отказам. В то же время избыточные компоненты (компьютеры, дисковые подсистемы) отнюдь не ограничиваются ролью горячего резерва — они полностью задействованы в процессе обычной работы.

Вся аппаратура устроена так, что допускает замену в горячем режиме, без остановки других компонентов кластера.

Кроме того устойчивый к отказам программный менеджер блокировок управляет параллельным доступом к базам данных. В результате обеспечивается целостность транзакций в сочетании с параллельной работой узлов кластера и с параллельным доступом к нескольким дисковым подсистемам. При этом выход из строя одного узла не означает краха всего сервера баз данных.

Подсистема обнаружения и нейтрализации отказов постоянно отслеживает доступность ресурсов, составляющих кластер. При обнаружении неисправности запускается процесс реконфигурации, изолирующий вышедший из строя компонент при сохранении работоспособности кластера в целом (с выходом из строя диска справляется менеджер томов).

Нейтрализация отказа узла (724)

Программное обеспечение предпринимает при этом следующие действия:

- Подсистема обнаружения отказов выявляет вышедший из строя узел.
- Создается новая конфигурация кластера, без отказавшего узла. Этот процесс занимает 1–2 минуты, в течение которых обработка транзакций приостанавливается.
- Менеджер блокировок производит восстановление. Подтвержденные транзакции от отказавшего узла (транзакции, об успешном завершении которых другие узлы кластера не успели узнать) накатываются вперед и деблокируются. Неподтвержденные транзакции от отказавшего узла откатываются и также деблокируются. В этот период транзакции обрабатываются исправными узлами, но, вероятно, несколько медленнее, чем обычно.
- Монитор транзакций повторно направляет в кластер неподтвержденные транзакции.
- Вышедший из строя узел ремонтируется и вновь запускается.
- Создается новая конфигурация кластера, включающая в себя отремонтированный узел.

Все действия, исключая ремонт отказавшего компонента, выполняются в автоматическом режиме и не требуют вмешательства обслуживающего персонала. Следует учитывать, однако, что если следующая поломка случится до окончания ремонта, кластер может на какое-то время стать неработоспособным, поэтому затягивать ремонт не рекомендуется.

Тиражирование данных (720)

В контексте информационной безопасности тиражирование можно рассматривать как средство повышения доступности данных. Стала легендой история про бакалейщика из Сан-Франциско, который после разрушительного землетрясения восстановил свою базу данных за 16 минут, перекачав из другого города предварительно протиражированную информацию.

В конфигурации серверов с тиражированием выделяется один основной и ряд вторичных серверов. На основном сервере выполняется и чтение, и обновление данных, а все изменения передаются на вторичные серверы, доступные только на чтение. В случае отказа основного сервера вторичный автоматически или вручную переводится в режим доступа на чтение и запись. Прозрачное перенаправление клиентов при отказе основного сервера не поддерживается, но оно может быть реализовано в рамках приложений.

После восстановления основного сервера возможен сценарий, при котором сервер становится вторичным, а бывшему вторичному, придается статус основного. При этом клиенты, подключенные к нему, продолжают работу. Таким образом, обеспечивается непрерывная доступность данных.

Тиражирование осуществляется путем передачи информации из журнала транзакций (логического журнала) в буфер тиражирования основного сервера, откуда она пересылается в буфер тиражирования вторичного сервера. Такая пересылка может происходить либо в синхронном, либо в асинхронном режиме. Синхронный режим гарантирует полную согласованность баз данных — ни одна транзакция, зафиксированная на основном сервере, не останется незафиксированной на вторичном, даже в случае сбоя основного сервера. Асинхронный режим не обеспечивает абсолютной согласованности, но улучшает рабочие характеристики системы.

Защита коммуникаций между сервером и клиентами (730)

Проблема защиты коммуникация между сервером и клиентами не является специфичной для СУБД, она присуща всем распределенным системам. Вполне естественно, что и решения применяются общие.

Ключевым компонентом в реализации взаимодействий клиент-сервер является сервис безопасности. Основные функции, предоставляемые этим сервисом, — аутентификация, авторизация (проверка полномочий) и шифрование.

Для каждого приложения клиент-сервер администратор может задать один из пяти уровней защиты:

- Защита пересылаемых данных только при установлении соединения клиента с сервером.
- Защита данных только на начальном этапе выполнения удаленного вызова процедуры, когда сервер впервые получает запрос.
- Подтверждение подлинности источника данных. Проверяется, что все поступающие на сервер данные получены от определенного клиента.
- Подтверждение подлинности источника и целостности данных. Проверяется, что отправленные данные не были изменены.
- Подтверждение подлинности источника, целостности и конфиденциальности данных. Выполняются проверки, предусмотренные на предыдущем уровне и осуществляется шифрование всех пересылаемых данных.

Сервис аутентификации существенно улучшает характеристики безопасности распределенной среды, упрощая в то же время деятельность как пользователей, так и администраторов. А наличие единой точки администрирования входных имен и прав доступа к базам данных и приложениям способствует упорядочению общей ситуации с безопасностью.

Защита ресурсных объектов (720)

С каждым объектом ИС связана некоторая информация, однозначно идентифицирующая его. Это могут быть число, строка символов, алгоритм, подтверждающие подлинность объекта. Определим такую информацию как идентификатор объекта. Процесс верификации этого идентификатора назовем идентификацией объекта. Если объект имеет некоторый идентификатор, зарегистрированный в сети, он называется легальным объектом; остальные объекты относятся к нелегальным.

Идентификация защищенного объекта — одна из функций подсистемы защиты, выполняемая в первую очередь, когда объект пытается войти в сеть. Если процедура завершается успешно, объект является легальным для данной сети. Следующий шаг — **верификация идентификатора объекта**, которая устанавливает, что предполагаемый легальным объект действительно таков, каким себя объявляет.

После того как объект идентифицирован и верифицирован, должны быть установлены сфера его и доступные ресурсы ИС. Такая процедура называется **предоставлением полномочий**. Перечисленные три процедуры инициализации относятся к единственному объекту ИС, и поэтому их следует отнести к средствам защиты самого объекта.

Особенности защиты персональных компьютеров обусловлены спецификой их использования. В большинстве персональных компьютеров отсутствуют совмещенные (многопрограммные) режимы работы, а в качестве носителя данных могут использоваться гибкие магнитные диски, компакт-диски, которые могут быть собственностью пользователя.

Если на ПК работает только один пользователь, то важно, *во-первых*, предупредить несанкционированный доступ к компьютеру других лиц в то время, когда в нем находится защищаемая информация, что возлагается на Службу охраны фирмы, а *во-вторых*, обеспечить защиту данных на внешних носителях от хищения.

Если ПК используется группой пользователей, то помимо указанных выше моментов защиты, может возникнуть необходимость предотвратить несанкционированный доступ этих пользователей к информации друг друга. Защита такого рода осуществляется с помощью специально разработанных программных средств.

При использовании персональных компьютеров в локальных или глобальных сетях возникают дополнительные задачи, например установление того, насколько обоснованно обращение к сети, опознавание пользователями предоставляемых им в сети вычислительных ресурсов, контроль безопасности сети. Решение этих задач осложняется такими факторами, как массовость персональных компьютеров, недостаточная квалификация и дисциплинированность некоторых сотрудников, высокая динамичность подключения и отключения от сети, большой объем выполняемых работ.

Система распределения обязанностей между отдельными служащими в значительной мере способствует повышению уровня сохранности информации, при этом целесообразно учитывать следующие принципы организации работ.

Минимизация сведений, доступных пользователям (723)

Каждый пользователь должен знать только те детали процедур обеспечения сохранности, которые необходимы ему для успешного выполнения своих обязанностей.

Данные, которые могут быть обозримы персоналом, ограничиваются. Так, отходы, в том числе черновики и копировальная бумага должны уничтожаться. Выходные данные, полученные на печатающих устройствах, должны предоставляться только тем, кому они предназначены. Обозначения носителей информации не должны раскрывать область их использования.

Минимизация связей пользователей (723)

Организация технологического процесса сбора и обработки информации и планирование помещений должны по мере возможности исключить или свести к

минимуму контакты персонала в процессе выполнения работ. Каждый сотрудник должен знать все о своей работе и связанных с нею ограничениях, а также четко представлять последствия нарушения этих ограничений.

Разделение полномочий

В информационных системах с высокими требованиями по обеспечению сохранности ответственная работа или процедура выполняется после подтверждения ее необходимости двумя сотрудниками. Например, можно потребовать, чтобы изменение полномочий пользователя осуществлялось только в том случае, когда руководитель и сотрудник, ответственный за обеспечение сохранности, одновременно послали в систему свои пароли с различных, специально выделенных для этой цели терминалов.

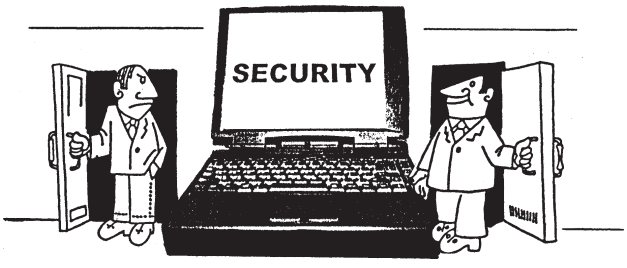
Дублирование контроля

Контроль важных операций никогда нельзя поручать одному сотруднику, так как бесконтрольное выполнение операций одним человеком может нанести ущерб сохранности информации. Присутствие еще одного сотрудника необходимо также и в соответствии с требованиями техники безопасности. Временные сотрудники или новички, а также сотрудники, проходящие обучение, не должны самостоятельно выполнять ответственные задания.

Контроль доступа

Мерой борьбы с целью предотвращения хищения информации является установление соответствующего контроля доступа в помещение, где размещается ПК.

Системы защиты должны разрешать пользователю при соответствующем контроле получать доступ к вычислительной технике и хранимой в ней информации. Для защиты от постороннего вторжения следует предусмотреть меры непосредственной защиты вычислительных устройств и информации от несанкционированного доступа.



Разделение полномочий...

Основными функциями, которые должны осуществлять в этих целях средства защиты, являются:

- идентификация субъектов и объектов;
- разграничение, а при необходимости — и полная изоляция доступа к вычислительным ресурсам и информации;
- регистрация действий в системе.

Процедура идентификации и подтверждения подлинности предполагает проверку, является ли субъект, осуществляющий доступ (или объект, к которому осуществляется доступ) тем, за кого себя выдает. В системах, обеспечивающих высокую безопасность, может потребоваться периодическая перепроверка подлинности.

В процедуре **идентификации** используются различные методы: простые, сложные или одноразовые пароли, обмен вопросами и ответами с администратором или через соответствующую программу; ключи, магнитные карты, значки, жетоны, средства анализа индивидуальных характеристик (голоса, отпечатков пальцев, геометрических параметров рук или лица), специальных идентификаторов или контрольных сумм для аппаратуры, программ и данных.

Совет

Наиболее распространенным методом идентификации является парольная идентификация. Надежность пароля зависит от его длинны. Рекомендуется использовать специальные средства генерации паролей и обеспечить надежное хранение пароля пользователем. В случаях, требующих высокой безопасности, используются одноразовые пароли.

После выполнения процедур идентификации и установления подлинности *пользователь получает доступ* к вычислительной системе, а защита информации осуществляется на трех уровнях: аппаратуры; программного обеспечения; данных.

Средства регистрации, как и средства контроля доступа, относятся к эффективным мерам противодействия несанкционированным действиям. Однако, если средства контроля доступа предназначены для предотвращения таких действий, то задача регистрации — обнаружить уже совершенные действия или их попытки.

Затраты, связанные с реализацией рассмотренных принципов, невелики. Однако они способствуют как повышению эффективности системы, так и обеспечению сохранности.

Защита физических объектов ИС (710)

Исторически сложилось так, что к моменту возникновения проблемы защиты информации средства охраны уже существовали. Однако следует помнить, что для

защиты информации и объектов, где она хранится, обрабатывается и циркулирует, используются более сложные и совершенные средства.

Определение

К техническим средствам охраны (ТСО) относят механические, электромеханические, оптические, акустические, лазерные, радиоволновые и другие устройства, системы и сооружения, предназначенные для создания препятствий на пути к защищаемой информации и способные выполнять функции защиты.

ТСО представляют собой первый рубеж защиты информации и элементов вычислительных систем, а поэтому обеспечение физической целостности таких систем и их устройств является необходимым условием защищенности информации.

Перечислим основные задачи, решаемые физическими средствами ЗИ:

1. Охрана территории;
2. Охрана внутренних помещений и наблюдение за ними;
3. Охрана оборудования и перемещаемых носителей информации;
4. Осуществление контролируемого доступа в защищаемые зоны;
5. Нейтрализация излучений и наводок;
6. Препятствие визуальному наблюдению;
7. Противопожарная защита;
8. Блокирование действий злоумышленника.

Защита объектов ИС заключается в создании интегрированных систем безопасности используемых информационных технологий.

Организационное построение СЗИ может быть представлено совокупностью следующих рубежей защиты: территории, здания (помещения), вычислительные ресурсы. При этом под рубежом защиты понимается организованная совокупность мероприятий, методов и средств, обеспечивающих безопасность объектов ИС. Некоторые характеристики и состав средств защиты представлены в таблицах 11.1–11.3.

Охранная и пожарная сигнализация (014)

Одним из основных средств обеспечения безопасности объектов являются системы сигнализации, которые должны зафиксировать приближение или начало действий самых разнообразных видов угроз — от пожара и аварий до попыток проникновения на объект или в компьютерную сеть.

Обязательной является пожарная сигнализация, которая представляет собой более разветвленную, чем другие виды сигнализаций, систему и обычно охватывает все помещения здания.

Пожарная и охранная сигнализации по своему построению и применяемой аппаратуре имеют много общего — каналы связи, прием и обработка информации, подача тревожных сигналов и др.. По этой причине в современных системах защиты обе эти сигнализации объединяются в единую систему.

Важнейшими элементами охранно-пожарной сигнализации являются извещатели, представляющие собой чувствительные элементы — датчики обнаружения изменений состояния среды и формирования извещения об этом. Характеристики датчиков определяют основные параметры всей системы сигнализации.

Контроль и управление охранно-пожарной сигнализацией осуществляются с центрального поста охраны, на котором устанавливается соответствующая стационарная аппаратура. Состав и характеристики этой аппаратуры зависят от важности объекта, сложности и разветвленности системы сигнализации. В простейшем случае контроль за ее работой состоит из включения и выключения извещателей, фиксации сигналов тревоги, проверки функционирования средств оповещения. В сложных, разветвленных системах сигнализации контроль и управление обычно осуществляются с помощью компьютеров.

Применение компьютерных систем охранно-пожарной сигнализации позволяет осуществить:

- управление и контроль за состоянием как всей системы, так и каждого извещателя (включен, выключен, тревога, выход из строя, сбой на канале связи, попытки вскрытия датчиков или канала связи);
- запись сигналов тревоги и документирование изменений состояния системы, служб охраны объектов;
- отображение ситуационного плана объекта, указание и подсказки к действиям персонала службы в соответствии с заранее разработанной тактикой охраны;
- возможность проведения “ситуационных игр” с целью обучения и отработки действий персонала службы охраны по защите объекта.

Критерием эффективности и совершенства аппаратуры охранно-пожарной сигнализации является сведение к минимуму числа ошибок и ложных срабатываний. Другим важным элементом является тревожное оповещение, которое в зависимости от конкретных условий должно передавать информацию с помощью звуковых, оптических или речевых сигналов (или их комбинацией). Тревожное оповещение имеет ручное, полуавтоматическое или автоматическое управление.

Таблица 11.1.

Наименование рубежа	Организационные меры защиты объектов ИС		
	Непосредственная защита	**Поддержание других средств**	**Объединение в СЗИ**
Охрана территорий	Контроль за прилегающей территорией, реагирование на сигнализацию о несанкционированном доступе на территорию и воздействия на нарушителя	Контроль состояния средств защиты	Контроль за соблюдением графика проведения организационных мероприятий по защите
Охрана помещений	Контроль санкционированности доступа пользователей и обслуживающего персонала в помещения путем проверки пропусков и отличительных знаков; совершенствование пропускного режима в выделенные помещения по результатам анализа регистрационных журналов и внезапных проверок, анализ журналов посещений с целью минимизации привилегий в доступе	Контроль реагирования системы сигнализации на попытки несанкционированного доступа в помещение	-«-
Защита вычислительных ресурсов	Регулирование доступа в помещение пользователей с помощью разработанных правил для пользователей путем внедрения единой системы пропусков; регистрация доступа пользователей, обслуживающего персонала к ПЭВМ; контроль за разграничением доступа пользователей к обработке информации в ПЭВМ	Контроль за модификацией программного обеспечения ПЭВМ с последующей его аттестацией	Регистрация и анализ проявления новых КНПИ; обеспечение постоянного контроля за пользователями с целью выявления несанкционированных потоков информации и копирования

Таблица 11.2.

Наименование рубежа	Технические средства внешней защиты объектов ИС				
	Охрана территорий	**Охрана помещений**	**Наблюдение**	**Разграничение доступа**	**Нейтрализация ЭМИ**
Охрана территорий	Механические преграды (забор), замки на воротах	-	Радиолокационные, теле-, фото-, лазерные, оптические системы видимой части спектра	Радиоуправляемые замки, механизированные и автоматизированные КПП	Устройства пространственного зашумления
Охрана помещений	-	Механические преграды (решетки, ставни), специальное остекленение окон, датчики огня, дыма, вредных веществ, системы пожаротушения	Теле-, фото-, ИК, акустические системы	Замки с кодовым набором, радиоуправляемые замки, замки, управляемые микропроцессором	Устройства изменения характера излучений
Защита вычисляемых ресурсов	Датчики различного типа, кабельные системы	Замки	Визуальные системы наблюдения за ПЭВМ, программно-аппаратная защита	Замки персональные микропроцессорные устройства проверки санкционированности доступа, устройства защиты полей запоминающих устройств	Экранирование устройств ПЭВМ, поглащающие экраны

Таблица 11.3.

Наименование рубежа	Программные средства защиты объектов ИС			
	Контроль	**Регистрация**	**Уничтожение**	**Сигнализация**
Охрана территорий	-	-	-	-
Охрана помещений	Контроль санкционированности доступа пользователей путем сравнения постоянного кода с кодом эталона	Регистрация доступа в помещение ПЭВМ пользователей методом ведения регистрации и накопления статистических данных в журнале по временным и количественным показателям	-	Сигнализация при попытках несанкционированного доступа в помещение ПЭВМ, при идентификации лиц, осуществляющих доступ
Защита вычислительных ресурсов	Контроль работы пользователя	Регистрация доступа с использованием ПЭВМ	Уничтожение остаточной информации в ЗУ ПЭВМ аварийное уничтожение информации в ОЗУ	-

Следует иметь ввиду что тревожное оповещение о возникновении пожара или других чрезвычайных обстоятельств должно отличаться от оповещения охранной сигнализации. Построение системы оповещения зависит от особенностей защищаемого объекта, его архитектуры и плана, характера производственной деятельности объекта, количества персонала, посетителей и др. При обнаружении угроз или чрезвычайных обстоятельств система оповещения должна содействовать организации эвакуации людей из помещений и зданий.

Каналами связи в системе охранно-пожарной сигнализации могут быть специально проложенные проводные линии, телефонные линии объекта и радиоканалы. Наиболее распространенными каналами связи являются многожильные экранированные кабели, которые для повышения надежности и безопасности работы сигнализации помещают в металлические или пластмассовые трубы, металлорукава.

Энергоснабжение системы охранной сигнализации должно обязательно иметь возможность резервирования. В случае выхода его из строя функционирование охранной сигнализации не прекращается за счет автоматического переключения резервного (аварийного) источника.

Технические средства, используемые в системах охранно-пожарной сигнализации (014)

Комплекс технических средств систем охраны в общем виде состоит из извещателей, шлейфов сигнализации, приемно-контрольных приборов, оповещателей.

При конструировании системы защиты одной из центральных задач является выбор оптимальных средств обнаружения и в первую очередь — датчиков охранной сигнализации. В настоящее время разработано и используется большое количество самых разнообразных извещателей охранной сигнализации.

Извещатель охранный (пожарный) — техническое средство для обнаружения проникновения (пожара), попытки проникновения или физического воздействия превышающего нормированный уровень, и фрмирования извещения о проникновении (пожаре). В охранно-пожарном извещателе совмещены охранная и пожарная функции.

В соответствии с ГОСТ 26342-84 извещатели классифицируются следующим образом:

- ***по назначению***: для открытых площадок и периметров; для закрытых помещений;
- ***по виду зоны, контролируемой извещателем***: точечные, линейные, поверхностные, объемные;
- ***по принципу действия:*** магнитоконтактные, ударноконтактные, пьезоелектрические, емкостные, ультразвуковые, оптико-электронные (активные, пассивные), радиоволновые, комбинированные;
- ***по количеству зон обнаружения:*** однозонные, многозонные;

По дальности действия ультразвуковые, оптико-электронные и радиоволновые извещатели для закрытых помещений бывают:

малой — до 12 м;

средней — от 12 до 30 м;

большой дальности — свыше 30 м.

По дальности действия оптико-электронные и радиоволновые извещатели для открытых площадок и периметров объектов бывают:

малой — до 50 м;

средней — от 50 до 200 м;

большой дальности — свыше 200 м.

По конструктивному исполнению ультразвуковые, оптико- электронные и радиозвуковые извещатели делят на:

однопозиционные — передатчик (излучатель) и приемник совмещены в одном блоке;

двухпозиционные — передатчик (излучатель) и приемник выполнены в виде отдельных блоков;

многопозиционные — более двух блоков (передатчики и приемники в любой комбинации);

Извещатели работают по принципу фиксации каких-либо изменений среды и делятся на:

объемные для контролирования пространства запретных зон и помещений;

линейные, или поверхностные, для контроля подходов к охраняемым объектам;

локальные, или точечные, для контроля отдельных предметов.

Извещатели, обнаруживающие угрозу пожара, реагируют на изменение среды под воздействием повышения температуры, появления дыма и других продуктов горения, возникновения светового излучения. В связи с многообразием условий в помещениях, подлежащих защите, на практике используется очень большое количество противопожарных датчиков. Некоторые типы извещателей, например, инфракрасные, используются одновременно и для охраны, и для обнаружения пожара.

Охранное видеонаблюдение (514)

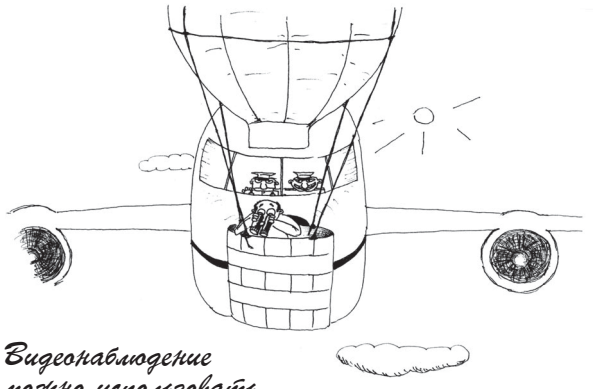
Многие читали или слышали о человеке по прозвищу "Соколиный Глаз". Интересен он не только тем, что был славным парнем, но и тем, что его зоркий глаз видел и различал врага издалека. Современные средства видеонаблюдения заменяют человеку несколько пар глаз и помогают видеть справа, слева и сзади.

Из истории

История фотоаппарата насчитывает чуть более 150 лет. Кино (прародителя видео) существует более 100 лет. История видео значительно моложе. Использование же видеонаблюдения в охранных целях получило развитие совсем недавно, хотя за короткое время сделало значительный рывок вперед, и стало одним из важнейших компонентов комплексных систем охраны.

Система видеонаблюдения это не дремлющее око охраны, круглосуточно обозревающее охраняемую площадь и запоминающее любые движущиеся объекты на ней.

Видеонаблюдение можно использовать практически везде — и в быту, и в бизнесе. Необходимость системы видеонаблюдения должны осознавать все. Пусть у вас будут заборы с колючей проволокой и пулеметами на вышках, охранники с собаками и автоматами, но наряду с этим необходима и система видеонаблюдения. Так, недавно на инкассатора-охранника одного из пунктов обмена валюты было совершенно вооруженное нападение. Два человека было убито, причем именно те, кто видел нападающего в лицо, а нападающий скрылся. Однако благодаря системе видеонаблюдения и видеорегистрации осталась запись действий преступника и были получены его фотографии. Помимо помощи, после нападения системы охранного видеонаблюдения позволяют также принять меры к недопущению преступления. Например, просматривая видеозапись, сотрудники службы безопасности выявляют наблюдение за объектом: наиболее часто проезжающая машина, человек или группа лиц, ведущие наблюдение.



Видеонаблюдение можно использовать практически везде...

Современные видеокамеры, применяемые в системах видеонаблюдения, используют в качестве "органа зрения" ПЗС (CCD) чипы. Эти чипы устроены таким образом, что позволяют "видеть" при слабой освещенности (свет луны), как днем. И более того, используя инфракрасную подсветку (невидима невооруженным глазом), можно наблюдать за охраняемой территорией в абсолютной темноте. При этом злоумышленник может думать, что невидим, а вы будете видеть его на мониторе, как днем. При этом система видеонаблюдения не устает и не теряет бдительность. Одна из фирм-производителей охранной видеотехники в рекламе задает вопрос: "Вы еще доверяете это дело людям?". И она права, люди могут ошибаться и предавать, техника же — никогда.

Компоненты и устройства видеосистем (514)

Современные системы видеонаблюдения могут быть различны по сложности: от камеры с монитором до многокамерных компьютерных систем с цифровой обработкой изображения в реальном масштабе времени. Конфигурация системы видеонаблюдения меняет-

ся в зависимости от конкретных задач. Однако как бы ни была сложна система видеонаблюдения, она обязательно содержит видеокамеру.

Видеокамера является источником изображения в системах охранного телевидения. Через объектив изображение предмета попадает на светочувствительный элемент камеры, в котором оно преобразуется в электрический сигнал, поступающий затем по кабелю на монитор.

В настоящее время разработано и выпускается большое количество типов и моделей видеокамер, которые можно классифицировать следующим образом:

- **видиконовые камеры** — в качестве светочувствительного элемента используется электронный прибор видикон. Камеры этого вида выпускаются давно; преимуществом их является низкая стоимость и простота конструкции. Недостаток — относительно короткое время службы (1–2 года) и малая чувствительность при низкой освещенности (5–10 люкс). Такие камеры в основном применяются для контроля за помещениями с постоянной освещенностью;
- **CCD камеры** — в качестве светочувствительного элемента используется специальный малогабаритный полупроводниковый сенсор (английское название CCD) Это относительно новый вид камер, которые имеют меньшие чем видиконовые камеры габариты, более высокую разрешающую способность и долговечность. Кроме того, CCD камеры могут работать при освещенности до 0,1 люкс и меньше. Стоимость таких камер достаточно высока.
- **сверхвысокочувствительные камеры** для работы при малой освещенности, практически в полной темноте;
- **специальные камеры** с инфракрасной подсветкой для наблюдения в ночное время без дополнительного внешнего освещения;
- **специальные малогабаритные камеры** для скрытного наблюдения через отверстие объектива не более 1–2 мм.

В последнее время начинают широко применяться цветные камеры, которые выгодно оличаются от черно-белых большей информативностью. Однако относительно высокая стоимость цветного видеооборудования несколько ограничивает сферы его применения.

Интересно

Все камеры охранного видеонаблюдения используют CCD кристаллы для передачи изображения. Кроме способности "видеть" в темноте, это позволяет миниатюризировать камеры и расширить их возможности. Одной из них является автоматическое электронное управление яркостью видеосигнала, называемое электронной диафрагмой (FC-55 и FC-65 фирмы "COMPUTAR"). Камеры, используемые в системах видеонаблюдения, как правило, черно-белые, поскольку это значительно уменьшает общую стоимость системы без снижения ее охранных качеств. Разрешающая способность видеокамеры обычно не превышает 330–400 телевизионных линий (в телевизоре 625 строк). Такая разрешающая способность дает достаточную четкость и позволяет идентифицировать человека с большого расстояния. Кроме того, важной характеристикой камер является размер CCD кристалла. Чем больше кристалл, тем больше "картинку" вы получите при прочих равных условиях. В охранной видеотехнике, как правило, используются камеры с размером CCD кристалла 1/3 и 1/2 дюйма. Стоимость стандартных черно-белых видеокамер 250–450 дол. США.

Важную роль "соколиного глаза" играет оптика видеокамер. На данный момент создано огромное количество объективов к видеокамерам, позволяющих видеокамерам полноценно функционировать.

Характеристики объективов во многом совпадают с фотографическими:

- длиннофокусные объективы используются для наблюдения за удаленными объектами или предметами небольшого размера;
- широкоугольные объективы устанавливаются там, где необходима панорама наблюдения за объектом;
- объективы с изменяемым фокусным расстоянием используются для приближения изображения объекта. Изменение фокусного расстояния осуществляется с помощью электронного дистанционного управления;
- объективы с автоматической (электронной) регулировкой диафрагмы устанавливаются в местах с большими изменениями освещенности. Это расширяет возможности наблюдения за объектами, как правило, вне помещения или в помещениях без дополнительного освещения в ночное время.

Важным показателем объективов является фокусное расстояние, от которого зависит как далеко и четко будет "видеть" камера. От фокуса зависит и угол зрения. Обычно чем больше расстояние, тем уже угол зрения (стоимость 20–120 дол. США). Существует большое количество моделей моторизованных объективов. По назначению они делятся на объективы с регулировкой диафрагмы (объектив с автодиафрагмой) и на объективы с изменением фокуса (трансфокаторы или zoom-объективы). Чем больше функций у объектива, тем он дороже. Объективы с автофокусом (стоимость 100–350 дол. США) лучше всего использовать в стационарных наружных камерах, где освещенность изменяется в широких пределах и электронная диафрагма камеры не может полностью компенсировать освещенность. Объективы с трансфокатором наиболее дорогие (600–1500 дол. США) и наиболее мощные устройства. Они позволяют изменять фокус, регулировать четкость изображения и оптимально подбирать диафрагму. Такие объективы наиболее пригодны для использования в камерах кругового обозрения совместно с поворотными устройствами. Например, для использования в людном помещении с несколькими входами. Одной камерой можно обозревать все помещение, рассматривать лица людей, выхватывая более крупное изображение или обозревать сразу большую площадь, но с более крупными деталями. Трансфокаторы обычно нуждаются в специальном устройстве управления — контроллере. Лучше всего использовать для камер объективы фирмы-изготовителя. Это объясняется более качественной работой и большей надежностью системы в целом. Однако есть всемирно известные фирмы-изготовители оптики, которые производят отличную продукцию для любых видеокамер (Rainbow).

Стоит также обратить внимание на аксессуары к видеокамерам. Для офисных камер практически ничего не требуется, а вот для внешних — необходимы герметичные корпуса, желательно с подогревом, для использования в суровых климатических условиях. Имеются "дворники" на корпуса и вспрыскиватели, но они, как правило, не применяются.

Совместно с трансфокаторами можно использовать поворотные устройства (800–1600 дол. США), что дает возможность сэкономить средства при необходимости обозрения широких пространств (складов или зон вокруг них).

Кроме обычных черно-белых видеокамер в охранном телевидении используются камеры с цифровой обработкой и управлением, а также — цветные камеры (CD-08 с цифровым управлением и встроенным объективом с трансфокатором).

Немаловажной частью видеосистем являются системы дистанционного управления камерами и устройства обработки видеоизображения. В этой области все чаще применяются микропроцессорные системы, которые дают пользователю удобный интерфейс, большое количество дополнительных функций и сервис. Наиболее часто применяемые устройства это мультиплексоры и контроллеры. Мультиплексоры делятся на два основных вида: с последовательным и одновременным выводом камер на экран. При использовании последовательных мультиплексоров "картинка" постоянно изменяется, и наблюдающий быстро устает. Поэтому лучше использовать мультиплексор с одновременным выводом на экран. При незначительном удорожании стоимости (300–500 дол. США для четырех камер) значительно увеличиваются возможности: на одном мониторе видно изображение сразу от четырех камер, на видеорегистратор записываются сразу все камеры, можно увеличить изображение с любой камеры, при тревоге автоматически включается изображение с нужной камеры, подается сигнал управления на видеорегистратор и при отключении сигнала от видеокамеры подается сигнал тревоги и показывается последняя поступившая картинка. Мультиплексоры, как последовательные, так и параллельные, могут иметь до 16 видеовходов (стоимость не более 5500 дол. США).

Контроллеры необходимы для управления поворотными устройствами и объективами с трансфокатором. Если используется более четырех камер с трансфокатором или поворотными устройствами, уместно применить систему телеметрического управления. То есть на камеры устанавливаются небольшие управляющие системы, а управление ведется от одного контроллера, который посылает сигналы управления любой камере. В достаточно сложных системах охранного телевидения используются специальные контроллеры типа KEY PRO, которые могут обрабатывать изображение и управлять камерами.

Кроме контроллеров используются видеодетекторы движения, которые обнаруживают движение, используя только сигнал с видеокамеры. Выпускаются устройства обнаружения движения, совмещенные с мультиплексором или в виде отдельного блока.

Монитор — второй по важности компонент после камеры. Монитор является вторым по значению элементом системы охранного видеонаблюдения. Конструкция монитора во многом схожа с конструкцией обычного телевизора. Отличие составляет то, что у монитора нет приемной части с помощью которой, подключив антенну настраиваются на прием телевизионных программ, передаваемых через эфир.

Сигнал от камеры с помощью кабеля подключается к блоку формирования изображения и далее к электронно-лучевой трубке.

Некоторые современные телевизоры имеют возможность работать и как телевизор и как монитор, но стоимость их значительно выше стоимости специализированного монитора с аналогичными возможностями просмотра изображений.

Мониторы различают по таким основным параметрам:

- размер экрана по диагонали (указывается в сантиметрах или дюймах). Наиболее распространенные размеры мониторов для систем охранного телевидения — 23 и 36 см;
- разрешающая способность, которая определяется максимально возможным количеством линий на экране монитора. Этот параметр монитора должен быть не хуже разрешающей способности камеры. Черно-белые мониторы имеют более высокую разрешающую способность, чем цветные (при одинаковых размерах экрана). Нормальной считается разрешающая способность 500−600 линий.

Выбор монитора для видеосистем...

Выпускаются мониторы для работы сразу с несколькими видеокамерами. Такие мониторы оборудованы устройствами автоматического переключения изображения последовательно от каждой камеры, через регулируемые промежутки времени, обычно от 1 до 30 с.

В некоторых типах мониторов предусмотрена возможность автоматического подключения камеры, в зоне обзора которой произошло срабатывание охранной сигнализации. Такие мониторы наиболее удобны при использовании большого числа видеокамер на сложных по конфигурации и числу помещений объектах.

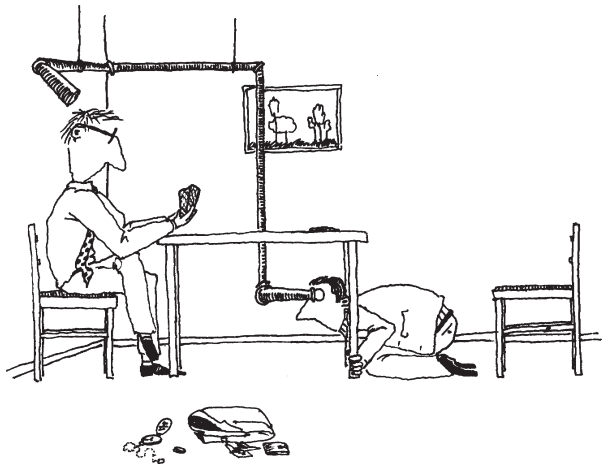
Разрабатывая систему видеонаблюдения следует учитывать, что чрезмерное увеличение количества мониторов приводит к снижению внимания работников охраны, повышению утомляемости и, соответственно, возрастанию вероятности ошибок. Практика показывает,что наибольшее внимание может быть сосредоточено на просмотре 4-х — 6-ти мониторов. Остальные мониторы должны обслуживаться другим охранником или работать в режиме включения от сигнализации.

Стоимость мониторов высока (200−350 дол. США), объяснение этому — высокая разрешающая способность. Для многокамерных систем используют 17- и 23-дюймовые мониторы, которые по своей разрешающей способности более чем в два раза превосходят телевизор (800−1500 дол. США).

Записывают изображение на видеорегистраторы — модернизированные видеомагнитофоны. Обычный видеорегистратор способен непрерывно записывать 24 часа на стандартную 3-часовую видеокассету (1200−1800 дол. США). Но и это не предел возможностей, модель CTR-960 фирмы COMPUTAR может записывать 960 часов (более 30 суток). При этом регистратор исправно записывает время и дату, а по сигналу тревоги переключается в специальный режим повышенного качества записи.

Дополнительное оборудование охранного видеонаблюдения расширяет его возможности и обеспечивает более оперативное и удобное использование всей системы. ***К дополнительному оборудованию относится***:

- видеокоммутатор — для подключения нескольких камер к одному монитору. Выбор камер производится вручную, путем нажатия соответствующей кнопки;
- автокоммутатор — для автоматического последовательного подключения камер к монитору или включения камеры по сигналу тревоги;
- формирователь изображения — для одновременного выведения изображений от 4-х камер на экран одного монитора (квадратор);
- детектор движения для подачи сигнала тревоги при возникновении каких-либо изменений в изображении, передаваемого от камеры. Детектор включается между камерой и монитором. Размер контролируемой зоны может регулироваться от полного экрана монитора до точки, наносимой на любой предмет изображения. ***По сигналу от детектора движения можно:***
  - автоматически подключать монитор к соответствующей камере для просмотра зоны, в которой произошло нарушение режима охраны;
  - подключать видеомагнитофон для записи изображения в зоне, где произошло нарушение режима охраны;
- включать тревожное оповещение для сигнализации сотрудникам охраны о нарушении режима охраны.



Дополнительное оборудование расширяет возможности...

Кроме стандартных видеокамер, в современных видеосистемах наблюдения все чаще используются скрытые и камуфлированные видеокамеры. Наиболее распространенные виды: картины, часы, пожарные и охранные датчики, зеркала, указатели выхода и др. Скрытое видеонаблюдение можно использовать для контроля лояльности сотрудников, соблюдения пропускного режима в подразделениях и регистрации переговоров. Для таких целей используются бескорпусные видеокамеры, размером 3–5 см. Существуют как черно-белые, так и цветные бескорпусные видеокамеры.

Для дома необязательно иметь сложную систему видеонаблюдения, достаточно поставить видеодомофон — переговорное устройство с видеокамерой. Одна часть видеодомофона устанавливается на двери, а вторая — в квартире. Когда посетитель нажимает кнопку звонка, сигнал вызова включает монитор, расположенный в квартире. Можно посмотреть на человека и переговорить с ним. При необходимости его впускают, открыв дверь с помощью электронного замка. Современные электронные и кодовые замки имеют специальные контакты для подключения к домофону. Кроме того, можно подключить камеру домофона к бытовому магнитофону или телевизору и контролировать входную дверь, не вставая с дивана. Видеодомофоны можно использовать как в квартирах, так и в офисах.

Компьютерные системы видеонаблюдения (614)

В системах видеонаблюдения достаточно часто используются мощные компьютерные системы и персональные компьютеры. На основе специализированных компьютеров строят системы распознания и идентификации видеоизображений, например системы доступа. Такие компьютеры могут функционировать автономно или замыкаться в компьютерную сеть и передавать данные на сервер, который хранит и ведет базу данных. Кроме мощных систем видеонаблюдения используются системы на базе обыкновенных персональных компьютеров. Такие системы могут хранить изображения людей, записывать изображение с видеокамер на различного рода накопители, выполнять контролирующие и обрабатывающие функции.

При всех трудностях использования компьютеров в системах видеонаблюдения пользователь получает доступ к современным информационным технологиям: автоматический поиск фрагментов записи, ведение баз данных, идентификация посетителей и многое другое. И хотя на данном этапе развития использование компьютеров в системах видеонаблюдения ограниченно, микропроцессорные устройства и информационные технологии все чаще вторгаются в эту область.

И все же, системы видеонаблюдения при всех своих огромных возможностях нуждаются в участии человека и всего лишь помогают ему.

Резюме

Файловые серверы могут контролировать доступ пользователей к различным частям файловой системы путем разрешения пользователю присоединить некоторую файловую систему (или каталог) к своей рабочей станции для использования как локального диска.

Это порождает две потенциальные проблемы.

Первая состоит в том, что сервер может обеспечить защиту доступа только на уровне каталога, поэтому если пользователю разрешен доступ к каталогу, то он получает доступ ко всем файлам, содержащимся в этом каталоге. Чтобы минимизировать риск в этой ситуации, важно соответствующим образом структурировать и управлять файловой системой ЛВС.

Вторая проблема заключается в неадекватных механизмах защиты локальной рабочей станции. Например, персональный компьютер может обеспечивать минимальную защиту или не обеспечивать никакой защиты информации, хранимой на нем.

Если информация, получаемая на основе конфиденциальных данных, предназначена для широкого использования, то требуют изменений правила управления потоком передаваемых данных. Это относится в первую очередь к статистическим базам и банкам данных, которые содержат конфиденциальную информацию об индивидуумах, используемую для формирования различных статистических сводок.

Особенность ситуации состоит в том, что сводки содержат “отголоски” исходной конфиденциальной информации, и весьма настойчивый пользователь может ее восстановить. Когда информация касается не-

которого конкретного индивидуума, процедура восстановления расценивается как посягательство на его личную тайну. Поэтому одна из задач процедур вывода состоит в том, чтобы стоимость восстановления конфиденциальной информации была исключительно высокой.

Проблема защиты коммуникация между сервером и клиентами не является специфичной для СУБД, она присуща всем распределенным системам. Вполне естественно, что и решения применяются общие.

Ключевым компонентом в реализации взаимодействий клиент-сервер является сервис безопасности. Основные функции, предоставляемые этим сервисом, — аутентификация, авторизация (проверка полномочий) и шифрование.

К техническим средствам охраны (ТСО) относят механические, электромеханические, оптические, акустические, лазерные, радиоволновые и другие устройства, системы и сооружения, предназначенные для создания препятствий на пути к защищаемой информации и способные выполнять функции защиты.

ТСО представляют собой первый рубеж защиты информации и элементов вычислительных систем, а поэтому обеспечение физической целостности таких систем и их устройств является необходимым условием защищенности информации.

Перечислим основные задачи, решаемые физическими средствами ЗИ:

1. Охрана территории;
2. Охрана внутренних помещений и наблюдение за ними;
3. Охрана оборудования и перемещаемых носителей информации;
4. Осуществление контролируемого доступа в защищаемые зоны;
5. Нейтрализация излучений и наводок;
6. Препятствие визуальному наблюдению;
7. Противопожарная защита;
8. Блокирование действий злоумышленника.

В системах видеонаблюдения достаточно часто используются мощные компьютерные системы и персональные компьютеры. На основе специализированных компьютеров строят системы распознания и идентификации видеоизображений, например системы доступа. Такие компьютеры могут функционировать автономно или замыкаться в компьютерную сеть и передавать данные на сервер, который хранит и ведет базу данных. Кроме мощных систем видеонаблюдения используются системы на базе обыкновенных персональных компьютеров. Такие системы могут хранить изображения людей, записывать изображение с видеокамер на различного рода накопители, выполнять контролирующие и обрабатывающие функции.