Хранение видеоданных: как повысить надежность?

Большинство современных систем видеонаблюдения, даже основанных на аппаратных видеорекордерах, позволяют сохранять архив, или периодически его копировать, или хотя бы копировать отдельные "тревожные" ролики на внешние носители. Рассмотрим, какие есть способы повысить надежность подсистемы хранения данных и когда они уместны

Алексей Омельянчук
Начальник КБ "Рубикон" компании "Сигма-ИС"

Для начала перечислим, как технически происходит запись на внешние носители. Аппаратные рекордеры, как правило, имеют мало возможностей. К некоторым может быть подключен внешний SCSI-накопитель, некоторые могут быть настроены хранить копию архива или отдельные тревожные ролики на Windows/Samba или на FTP-файловом сервере, некоторые могут (как правило, речь только про тревожные короткие ролики или даже только про отдельные кадры) отправлять эти ролики по E-mail или загружать по http. Кроме того, многие рекордеры поддерживают потоковую трансляцию видео по сети, так что соответствующее программное обеспечение на специальном сервере может самостоятельно сохранять видеоархив. В таком случае мы фактически имеем дело с PC-based-рекордером, который обычно предоставляет куда более широкие возможности по настройке хранения. Может применяться любое средство хранения, которое можно использовать с компьютера под соответствующей операционной системой.

Повышение надежности в видеонаблюдении

Теперь посмотрим вокруг – какие средства повышения надежности хранения данных выработаны ИТ-индустрией для задач общего назначения и какие могут быть применены в видеонаблюдении.

Во-первых, существуют жесткие диски и серверные платформы повышенной надежности. Большой запас мощности блока питания, активное охлаждение дисков и процессора, применение комплектующих, условно говоря, "девятой приемки" и схемотехники с многократным запасом прочности. Этот способ был исторически первым, но сейчас в реальности он последний, когда уже все остальное сделано и хочется повысить надежность с 99,99 до 99,999% за любые деньги. Такие решения очень дорогие, цена особо надежных комплектующих примерно на порядок превосходит обычные, а выигрыш в надежности не так уж и велик (срок службы вырастает в 2–3 раза, но вряд ли это кого всерьез беспокоит – все компьютерные комплектующие морально устареют раньше). Единственное реальное достоинство высоконадежных комплектующих – более или менее гарантированная надежность в первые дни эксплуатации (за счет тщательного выходного контроля отбраковываются изделия с легко проявляющимися скрытыми дефектами, именно такие дефекты дают повышенную частоту отказов в начале эксплуатации обычных изделий).

Технология RAID

Самый распространенный способ повышения надежности – резервирование. Знаменитая технология RAID (Redundant Array of Inexpensive Disks – резервированный массив недорогих дисков) обеспечивает продолжение работы дискового массива при выходе из строя одного любого диска. Вероятность одновременного выхода из строя сразу двух даже самых дешевых дисков намного ниже, чем вероятность отказа одного, пусть даже самого дорогого, диска. Уточню, что слово "одновременного" означает "пока не заменили предыдущий". То есть ключевым моментом в таком случае оказывается быстрая замена вышедших из строя дисков. Иначе никакого выигрыша вы не получите вовсе. Кстати, равно бессмысленно обеспечивать время в несколько секунд на замену диска, само по себе восстановление информации после установки нового диска обычно занимает несколько часов. И помните, термин RAID нынче не означает наличия резервирования. Есть решения, также называемые RAID, которые предназначены для ускорения работы дисков (RAID 0), они, наоборот, сильно снижают надежность – достаточно выйти из строя одному из дисков, и все данные потеряны. Защиту обеспечивают RAID 1 и выше, самый распространенный вариант – RAID 5.

Еще более изощренные решения предполагает распределенный "кластер" серверов, объединенных отказоустойчивой сетью (для информации – в сетевых технологиях аналогом RAID является Spanning Tree, кому нужны подробности – Яндекс в помощь).

SAN и NAS: в чем отличия?

Опишу подробнее, какие виды сетевых хранилищ встречаются и чем они отличаются. Во-первых, самая большая разница между терминами с минимальным отличием – SAN и NAS. Первый – SAN (Storage Area Network) – предоставляет компьютеру (или, в нашем случае, видеорекордеру) доступ к блочному хранилищу. То есть обеспечивается хранение абстрактных блоков информации, как на обычном жестком диске. Это теоретически позволяет использовать такое хранилище из любой программы, даже ориентированной на прямую запись на диск (так ведут себя многие рекордеры, даже PC-based), а с применением аппаратных конвертеров теоретически даже подключить к железным (non-PC-based) видеорекордерам. Учтите, что Windows имеет очень ограниченные возможности поддержки SAN (только iSCSI и только начиная с версии 7).

Второй тип сетевых хранилищ – NAS (Network Attached Storage) – это широко распространенные файловые серверы, на которые можно писать и с которых читать отдельные файлы. Обратите внимание, чаще всего сетевым хранилищем называют именно файловые серверы.

Что касается резервирования (повышения надежности хранения данных), то в обоих случаях резервированными могут называться как устройства, просто-напросто имеющие RAID-массив дисков, так и кластеры (группы) устройств в сети, которые могут быть изрядно разнесены пространственно.

Итак, теперь рассмотрим, от каких угроз какие меры повышения надежности имеет смысл применять.

Защита от главных угроз

Угроза первая – аппаратный сбой. Если вас беспокоит только невысокая надежность аппаратуры, скорее всего, достаточно организовать RAID-массив дисков. Этого хватит, чтобы основной проблемой надежности стал вопрос – как защититься от сбоя собственно рекордера, каков бы он ни был. Реально это возможно только за счет уменьшения размера рекордера – если один рекордер записывает только одну камеру, то при отказе этого рекордера пропадет запись лишь от одной этой камеры (как, впрочем, и при отказе самой камеры).

Для IP-камер можно рекомендовать применить резервирование в виде локальной записи на самой камере (то есть выбрать камеры с такой возможностью) – там обычно небольшой объем хранилища, но его должно быть достаточно на время, пока вы не замените центральный рекордер. Еще возможно резервировать рекордер, хотя это может быть непросто. Аналоговые камеры следует запараллелить (или разветвить специальным усилителем) на два рекордера, это понятно. А вот IP-камеры не всегда легко настроить так, чтобы они посылали видеопоток на два рекордера одновременно. Обычно для этого необходимо применять режим широковещательного (Broadcast) или многоканального (Multicast) вещания, что потребует также осторожной настройки сети передачи данных (коммутаторов).

Угроза вторая – сознательное повреждение аппаратуры преступниками. Это серьезная угроза для автономной системы видеозаписи на объекте без круглосуточной охраны, или

если вооруженные нападающие подавили сопротивление охраны. Решения возможны различные, лучше всего применять сразу несколько из них.

Например, обеспечить хранение данных вне объекта – построить систему в стиле VSaaS, когда камеры стоят на объекте, а все центральное оборудование где-то в специальной организации, и передача данных происходит по Интернету или по специальным выделенным каналам. Недостаток такого решения – вместо повреждения аппаратуры записи преступникам достаточно заблаговременно перерезать линию связи, что может оказаться даже легче. Конечно, следует предусмотреть наличие нескольких каналов связи, в том числе и по сотовой сети.

Помните, помимо полностью облачного решения возможны и различные гибридные, когда запись ведется в основном локально и лишь тревожные фрагменты пересылаются на внешний сервер. Огромное количество программных и аппаратных рекордеров умеют обеспечивать пересылку в Интернет тревожных записей. Причем для этого необязательно заключать договор со специальной организацией – может использоваться обычный арендуемый в датацентре FTP-сервер или даже файловый сервер в офисе дружественной компании.

Еще один способ защититься от сознательного повреждения аппаратуры – разместить ее в специальном сейфе, несгораемом и непотопляемом. Удобнее это сделать именно с компактным сетевым хранилищем, чтобы не ставить большой рекордер, кодер аналоговых сигналов и мощный компьютер с видеоаналитикой. Достаточно вынести только файловый сервер, разумеется, с резервированным дисковым массивом (RAID 5). Его можно спрятать в труднодоступное место да еще и в огнестойкий сейф со встроенной системой кондиционирования.

Наконец, некоторую защиту дают локальные хранилища на IP-камерах. Ободрать со стен на высоте 4 метра десяток камер намного сложнее, чем разбить (или унести с собой) один видеорекордер, стоящий на столе в вестибюле.

Следующая угроза – искажение данных в хранилище. Недобросовестный сотрудник охраны может при желании стереть некоторые данные или даже подделать их, подменив данные за вторник аналогичным периодом за понедельник. Цифровые записи, в принципе, подделать возможно. Вопрос в наличии времени и средств. Поэтому, кстати, и в суде трудно использовать записи, про которые никто не может сказать, где и как они хранились.

Что можно посоветовать? Конечно, обязательно хранить резервную копию вне объекта охраны, иначе, даже если не получится подделать или стереть данные, мерзкий предатель "нечаянно" прольет на видеорекордер кофе или уронит огнетушитель. При этом копия должна быть именно резервной копией, с которой невозможно осуществить никакие действия с помощью штатных органов управления системой. Самый лучший вариант: если потенциально важные ролики будут как можно быстрее (например, непосредственно сразу после обнаружения тревоги и экспорта тревожного ролика) загружены на независимый авторитетный сервер. Справка от Google, что этот файл лежит на Google Drive с такого-то числа без изменений, будет положительно воспринята судом, если возникнет необходимость.

Итак, в этой статье описаны некоторые принципы повышения надежности хранения видеоданных, наработанные в ИТ-индустрии, и приведены основные ключевые слова, по которым можно искать информацию дальше. В целом современное состояние компьютерных технологий позволяет обеспечить исключительно высокую надежность как при локальном хранении данных, так и при пересылке данных в удаленные хранилища. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru