Банк

Финансовые учреждения подвержены различным опасностям и перманентным рискам. Мошенничество с банкоматами, вандализм, разбойные нападения и кражи со взломом – это, к сожалению, повседневные явления. Все эти преступления требует принятия мер превентивной защиты финансовых учреждений для отпугивания потенциальных преступников и в необходимых случаях для их быстрого изобличения с убедительными доказательствами.

Выдача наличных денег в банкоматах в помещениях банков или на открытом пространстве возле их зданий – здесь сбором доказательств преступлений должны заниматься сами банки, даже вне их рабочего времени. Такие преступления, как махинации с банковскими картами или нанесение ущерба вандалами, редко раскрываются без средств видеонаблюдения, без которых они требуют крупных расходов и затрат на персонал.

Разбойные нападения – существует ли большая опасность для служащих и клиентов финансовых учреждений? Во всех финансовых учреждения России, в которых принимаются или выдаются банкноты, действуют инструкции по работе с наличными деньгами. Эти инструкции обязывают владельцев учреждений оснащать помещения необходимыми средствами контроля и определяют минимальные технические характеристики оборудования видеосистем безопасности – от разрешения изображений, углов обзора камер видеонаблюдения, скорости и длительности записи изображений, до периодов профилактики оборудования.

Кражи со взломом и действия вандалов происходят, как правило, вне рабочего времени, по ночам или в конце недели. В это время служащие в финансовом учреждении отсутствуют. Круглосуточное присутствие персонала охраны на местах стоит дорого. Оперативные силы быстрого реагирования по тревогам не знают заранее, что их ожидает ...

Решения для видеосистем безопасности, которые отвечали бы требованиям инструкций по работе с наличными деньгами, автоматически выдавали бы тревоги, передавали бы информацию обо всех происшествиях в ситуационный центр, или просто документировали бы ее для последующего анализа.

Гибридный рекордер является идеальной комбинацией цифровых и аналоговых решений для банковских систем видеонаблюдения. Он обрабатывает как аналоговые сигналы камер, так и видеоданные IP-камер или мегапиксельных камер. Благодаря модульности и сетевым характеристикам устройства, его можно объединять в сети вместе с рабочими станциями для операторов.

Пример:

Запись процесса выдача наличных денег в банкоматах

Управление устройством производится системой контроля доступа банка (входная дверь в фойе) и банкоматом, при этом запись изображений с камер видеонаблюдения управляется событиями по предварительной настройке конфигурации событий.

Процедура выдачи наличных денег клиенту документируется следующим образом:

- Состояние покоя, непрерывно записываются изображения с камер видеонаблюдения в фойе (со скоростью 2 кадра в секунду, с предысторией событий продолжительностью 2 минуты).
- Считыватель карт у двери в фойе считывает данные с карты клиента.
- Считыватель карт передает данные входящего клиента (опция: вместе с банковскими реквизитами и номером счета) и запускает этим запись события.
- Скорость записи камер видеонаблюдения в фойе увеличивается до 6 кадров в секунду. Дверь открывается.
- Клиент приближается к банкомату (опция: датчик движения у банкомата подает сигнал тревоги).
- Банковская карта вставляется в считыватель карт банкомата, начинается запись изображений посетителя анфас камерой видеонаблюдения.
- Банкомат отрабатывает процедуру снятия денег и передает номер счета и реквизиты банка вместе с текущими датой и временем.
- С начала процедуры выдачи денег производит запись изображений дополнительной камеры видеонаблюдения направленной на руки клиента, берущего деньги.
- Изображения камер видеонаблюдения в фойе продолжают записываться до тех пор, пока клиент не покинет фойе.

Все видеозаписи привязаны к данному событию выдачи денег клиенту вместе данными даты/времени, банковских реквизитов и номера счета в качестве критериев для поиска.

События могут храниться несколько месяцев в архиве на фиксированных носителях данных в зависимости их емкости, при необходимости их можно копировать на мобильные носители данных, например, DVD-диски. Процесс поиска записанных данных в архиве может производиться параллельно и независимо от процесса записи текущих изображений, как локально в самом устройстве, так и по сети.

Пример: Разбойные нападения, требования для банковских и кассовых систем
Запись разбойных нападений согласно требованиям к безопасности для банковских и кассовых систем:
Формулируются требования к оборудованию видеосистем безопасности для финансовых учреждений следующим образом:

- Камеры видеонаблюдения в кассовых помещениях финансовых учреждений должны быть установлены так, чтобы они позволяли фиксировать и документировать на видеозаписях характерные приметы злоумышленников, например, телосложение, одежду, движения и т.п., на сцене шириной максимум 6 метров для каждой камеры.
- Зона перед кассами должна охватываться камерами видеонаблюдения с максимальной шириной сцены 1,5 м, чтобы можно было распознать лица злоумышленников, или, были отчетливо заметны другие приметные детали, если лица закрыты маской.
- Дополнительно рекомендуется включать в тревожные видеозаписи изображения различных камер в помещениях финансовых учреждений, чтобы получить возможность записи вероятных моментов надевания или снятия масок.
- Качество изображений во всей видеосистеме (разрешение в пикселях, цветовые характеристики, распознаваемость деталей, качество записи) должно соответствовать тестовой таблице, прилагаемой к требованиям к безопасности для банковских и кассовых систем.
- Запись разбойных нападений должна включать в себя запись их „предыстории“ продолжительностью 15 минут до выдачи сигнала тревоги. Скорость записи изображений для каждой камеры должна составлять 1 кадр в секунду.
- После поступления сигнала тревоги о разбойном нападении должна производиться запись изображений всех камер видеонаблюдения в течение следующих 15 минут со скоростью 2 кадра в секунду.
- Все видеозаписи разбойных нападений должны быть защищены от записи, манипуляций, и копирования посторонними лицами.
- В системе должна быть предусмотрена возможность копирования на компакт-диски видеозаписей разбойных нападений и их отображения стандартными средствами на экранах мониторов персональных компьютеров.

Видеорекордер сертифицирован согласно требованиям к безопасности для банковских и кассовых систем, отвечает всем необходимым характеристикам и может многое другое:

- Видеозаписи тревог и разбойных нападений имеют статус защищенных от записи все время, пока этот статус не отменен.
- 15-минутные видеозаписи предысторий, выделяемые из перманентно записываемых данных в соответствующий циклический буфер, автоматически включаются в видеозаписи разбойных нападений.
- Для видеозаписей тревог можно вручную отменять статус защиты от записи только после сохранения их в архивах на внешних носителях данных, их просмотра несколькими пользователями.
- Функция автоматического архивирования, благодаря предварительной настройке конфигурации событий, позволяет копировать видеозаписи тревог на дополнительные носители данных, сетевые или в специально выделенной центральной базе данных.
- Нажатием кнопки на передней панели устройства видеозапись последней тревоги может быть скопирована на предварительно подключенный к порту USB сменный носитель данных, например, компактный диск CD, DVD или модуль флеш-памяти.
- Все экспортированные изображения и последовательности кадров снабжаются цифровой подписью и содержат дополнительную информацию о том, какой прибор, когда и что записывал. Эта информация параллельно заносится во внутренний системный журнал.
- В устройстве записи изначально сконфигурированы следующие тревожные контакты:
  - Контакт 1 = контакт сигнала разбойного нападения, по которому запускается запись изображений всех камер со скоростью 2 кадра в секунду, а также прикладывается видеозапись предыстории разбойного нападения, выделенной из перманентно записываемых данных в соответствующий циклический буфер.
  - Контакт 2 = контакт сигнала предварительного предупреждения (предтревоги, подозрения), по которому запускается запись изображений всех камер со скоростью 2 кадра в секунду.
  - Контакты 3 – 16 конфигурируются произвольно.

Пример: Кражи со взломом

Запись процесса кражи:

В не рабочее временя устройство записи с помощью свободно программируемого **управления по расписанию** переключается на полностью автоматический режим работы.

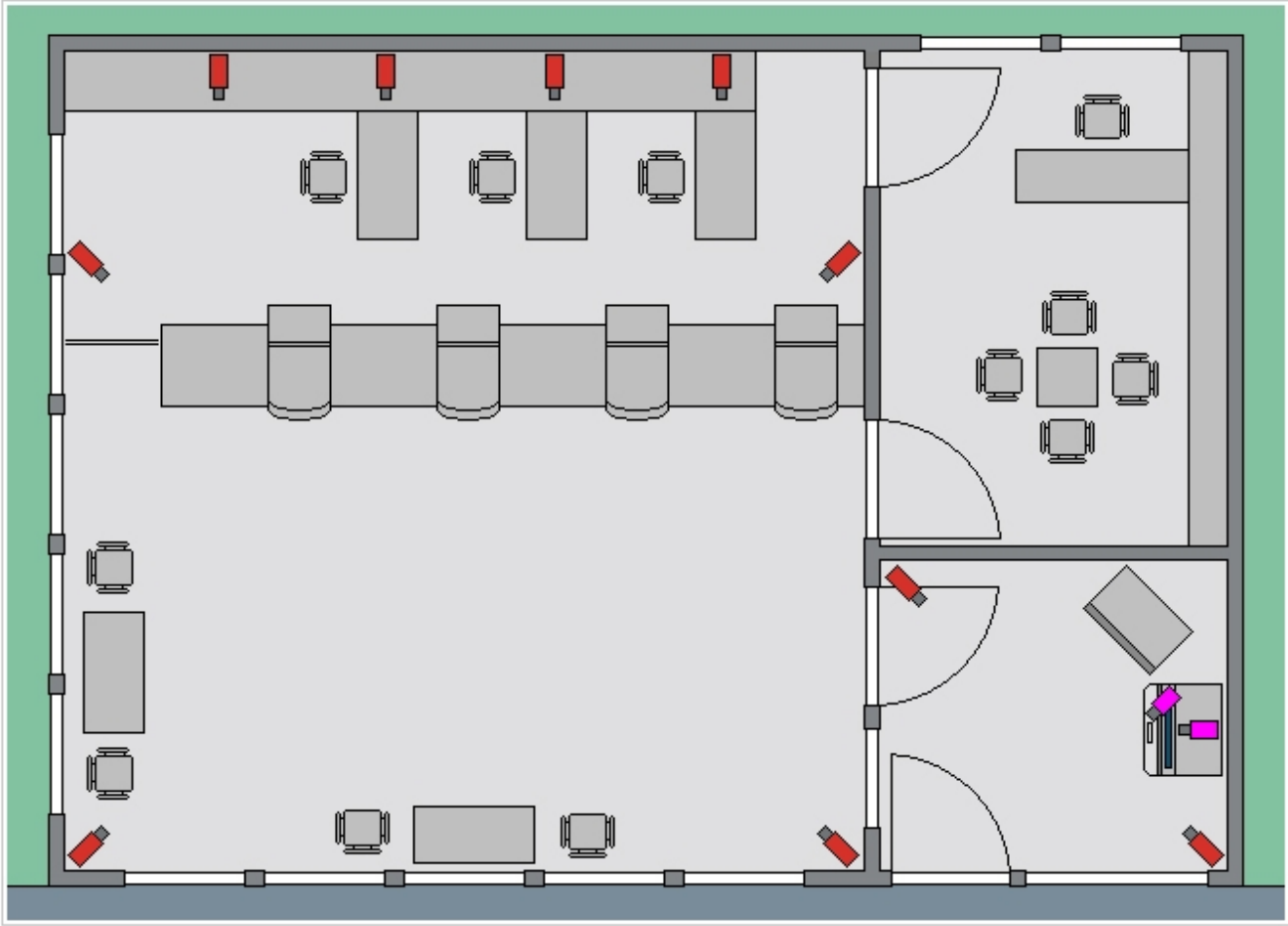
Для видеонаблюдения в особо охраняемых зонах, таких, например, как коридоры, помещения сейфовых хранилищ (ночью в них включается аварийное освещение) активируется функция детектирования активности по алгоритму AD. Запись изображений управляется событиями по сигналам тревог, срабатыванию дверных контактов или датчиков разбития стекла. Отказы камер видеонаблюдения, изменения направления обзора камер или открытие корпуса, распознаются и сигнализируются автоматически с помощью функции контроля положения камеры.
Встроенная функция обработки аудио сигналов позволяет не только передавать и записывать звуки параллельно с изображениями, но и выдавать сигнал тревоги при возникновении непривычно громких шумов, таких, например, как звон разбитого стекла или шум механизмов.

В случае тревоги устройство записи параллельно с записью изображений автоматически устанавливает сетевое соединение с центральным постом охраны и передает туда тревожные кадры. Один охранник центрального поста охраны в состоянии централизованно контролировать несколько охраняемых финансовых учреждений, быстро оценивать изменения обстановки и оперативно принимать соответствующие меры.

Охранник, находящийся на центральном посту охраны, имеет возможность в любой момент времени совершить „электронный обход“ охраняемого объекта. Он также может с помощью выходных управляющих контактов устройства дистанционно включить свет в помещении, выбрать камеру для вывода ее изображений на монитор, и при необходимости управлять имеющимися подвижными камерами.

Встроенные средства диагностики распознают вероятные ошибки системы и сообщают о них средствами оповещения по протоколу SNMP. „Электронный обход“ охраняемого объекта, удаленная передача изображений, включение освещения в любой момент времени возможны также с удаленных рабочих мест.

Пример: Графический план филиала банка.



Bank 11.10.2010