УДК 654.9

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ ОХРАННЫХ СИСТЕМ БЕЗОПАСНОСТИ БАНКОВСКИХ УЧРЕЖДЕНИЙ

Д.В. Бычков, В.В. Надвоцкая
Алтайский государственный технический университет им. И.И. Ползунова
г. Барнаул

Статья посвящена технологии проектирования систем безопасности на основе требований к оборудованию банковских учреждений.

Ключевые слова: охранные системы, рубежи сигнализации, авторизованный контроль.

В банках, работающих с физическими лицами, требования к охранным сигнализациям заведомо более серьезны, чем в большинстве организаций, относительно как повышенного уровня защищенности, так и конкретных эксплуатационных процедур. Безопасность банка включает в себя не только защиту клиентов и работников банка, целостность имущественного состояния банка, но и также неприкосновенность информационных средств. Система безопасности включает в себя три основные части - видеонаблюдение и прочность окон и дверей, круглосуточная охрана, программная безопасность [4].

В данной работе рассмотрим нюансы охранных мер, исключая информационную и программную безопасность. При проектировании систем необходимо учитывать такие факторы, как надежность; удобство и простота в использовании.

Все устройства мониторинга находятся в здании банка, а именно в пункте охраны и у сотрудников службы безопасности (отображение видеонаблюдения). Пункта охраны в случае «тревоги» передается сигнал на центральный пункт охраны, где диспетчер сообщает группе быстрого реагирования – ГБР.

При проектировании охранной системы банка первой задачей является оценка возможной угрозы, для чего создаются рубежи сигнализации - совокупности технических средств охраны, позволяющих выдать адресное извещение о проникновении на отдельные номера пультов центрального наблюдения или приемно-контрольных приборов, размещенных в пунктах централизованной охраны. Первый рубеж - защита строительных конструкций периметров помещений, оконные и дверные проемы, люки, вентиляционные каналы, тепловые вводы, тонкостенные перегородки и другие элементы помещений, доступные для проникновения с внешней стороны, в т.ч. и тех из них, которые оборудованы стальными решетками. Второй рубеж - с помощью специальных приборов охранной сигнализации защищаются помещения внутри здания. Третий рубеж - перекрывает охраняемые хранилища внутри помещений, средства и материальные ценности. При наличии в охраняемых помещениях нескольких рубежей сигнализации каждый из них создается и вещателями, работающими на различных физических принципах.

Система охранных мер должна предусматривать устойчивую (дублированную) систему связи и управления связи всех взаимодействующих в охране структур.

В пример этого рассмотрим передачу данных на пост охраны с кассового узла, который сначала берется под охрану независимо, а после на посту охраны. Передача информации может реализоваться двумя методами: по линии и GSM. Используя оба метода, мы добиваемся дублирования сигнала и в случае нарушения одного из способа связи, работоспособность продолжается. Также использование топологии «кольцо» в охранной сигнализации является дублированием, в случае обрыва цепь продолжает функционировать. Аппаратура охранной, охранно-пожарной и тревожной сигнализации, телевизионные системы охраны и наблюдения, системы контроля управления доступом могут быть объединены в единый комплекс технических средств охраны учреждения банка. Вывод информации с составных частей комплекса технических средств охраны осуществляется на центральный пункт управления или отдельные пульты управления систем [3].

В данной работе предлагается техническое решение на основе адресных

датчиков и приборов для отслеживания срабатывания системы. При решении технических задач охраны в первую очередь необходимо выбрать основные параметры устройств, которые обеспечат достаточную надежность выполнения возложенных на них функций. С помощью систем ограничения доступа осуществляется автоматизированный контроль доступа в помещения. Это могут быть небольшие системы на 1-3 двери и системы, контролирующие перемещение до нескольких десятков тысяч человек. Ограничение доступа должно осуществляться без потерь времени и при этом обеспечивать надежный контроль. Идентификация пользователя происходит посредством магнитной или электронной карточки. На особо ответственных участках система контроля дополняется набором кода (рисунок 1).

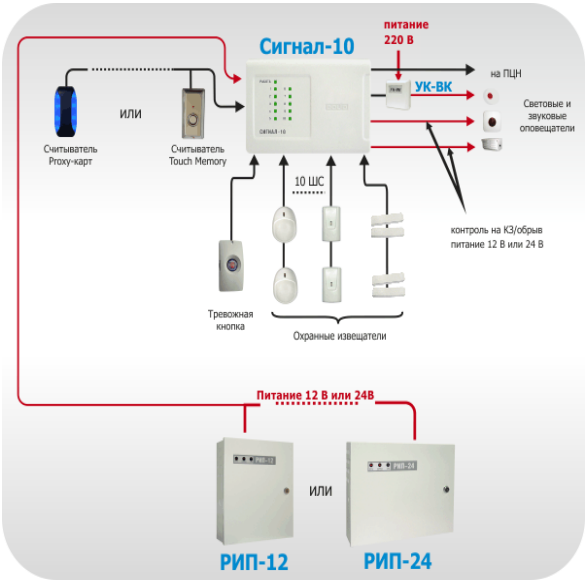

Рисунок 1 – Схема подключения контроллера "С2000-2" в режиме "Одна дверь на вход/выход"

С помощью магнитных датчиков формируются сообщения "Проход" при срабатывании этой цепи. Таким образом будет производится контроль за дверьми и окнами. Магнитные датчики относятся к самым простым и устанавливаются на окна, двери и люки. Выпускаются двух видов: для наружной и скрытой установки. Обычно размещаются в верхней части двери или окна. С целью повышения надежности устанавливается по два датчика, соединенных последовательно. При установке на окнах каждая фрамуга окна защищается парой <геркон + магнит>.

Электромагнитные замки вместе с доводчиками реализуют закрытие дверей. Считыватели совместно с электромагнитным замком организуют открытие/закрытие дверей, а также помогут отслеживать кто именно, когда и где проходил. Считыватели системы монтируют в двери, рамы двери, перегородки/стены и кабины лифта таким образом, чтобы они были легко доступны. В оформлении считывающих элементов учитываются эргономические и эстетические требования. Ядро системы располагается на защищенном участке [2].

Ручные охранные извещатели ("тревожные кнопки") передают на пульт мониторинга тревожный сигнал вне зависимости от того, поставлена ли система на охрану. Подать сигнал тревоги с их помощью можно рукой или ногой. Надежность охранных устройств непосредственно определяется работоспособностью бесперебойного источника питания. Он должен обеспечивать электропитанием все элементы охранных систем, для этого они должны быть промышленные и несколько. При разветвленной схеме системы безопасности, происходит распределение резервных источников питания (РИП). Они обеспечивают электроэнергией группы близко расположенных охранных устройств.

Все выше перечисленные устройства подключаются к приборам серии BOLID, а именно Сигнал - 10, которые будут управлять работой датчиков и механизмов, а так же передавать данные на центральный пульт. С ним в свою очередь будет связан клиент в виде персонального компьютера [1]. Это позволит совместить проект здания со всем охранным оборудованием, что весомо упростит как мониторинг, так обслуживание.

Отображаться результаты работы всей цепочки охранного оборудования будут с помощью специализированного программного обеспечения, подразделяемого на три уровня: приборный, пультов управления (сетевое взаимодействие между автономными устройствами, индикация событий, управление автоматикой, зонами и выходами устройств), системное (организация автоматизированных рабочих мест с функционалом мониторинга и управления). Программное обеспечение также учитывает требования банковского учреждения: введение временных задержек при доступе в критически важные зоны,

функция регистрации действий по силовому демонтажу банкомата, обеспечение максимально раннего оповещения, если есть подозрение попытки проникновения через стену [5].

Таким образом, рассмотрены основные аспекты проектирования охранных систем для банковских учреждений в разрезе требований к оборудованию банковских учреждений инженерно-техническими средствами в отношении надежности охраны, пропускного режима и технической укрепленности банка.

Продолжением проекта может стать разработка многофункционального продукта, интегрированного с системами управления инженерными сетями здания, и позволяющего, например, автоматически выключать свет и понижать уровень отопления при постановке на охрану.

СПИСОК ЛИТЕРАТУРЫ

1. Bolid – приемно-контрольные приборы, извещатели, оповещатели. [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://bolid.ru – Загл. с экрана.

2. Krystal: специализированное предприятие по разработке и изготовлению средств связи [Электронный ресурс]. – Электрон. дан. – Режим доступа http://www.ksytal.ru. – Загл. с экрана.

3. Mostok 2008: техническая поддержка [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.mostok2008.org – Загл. с экрана.

4. Концепция безопасности коммерческого банка // Информационный портал по охране и безопасности [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://specialsecurity.biz/publ/koncepcija_bezopasnosti_kommercheskogo_banka/24-1-0-49. – Загл. с экрана.

5. Охранная сигнализация для банка // Security News [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.secnews.ru/articles/16744.htm#ixzz2hiIGG7dU. – Загл. с экрана.

Надвоцкая Валерия Валерьевна – доцент, тел.: (3852) 290-913, e-mail: nadvotskaya7@mail.ru; Бычков Дмитрий Владимирович – студент.