

ОБЩИЕ РЕКОМЕНДАЦИИ ПО ВЫБОРУ ОХРАННОЙ СИСТЕМЫ

При выборе системы безопасности для охраны квартиры, дома или офиса, необходимо определить задачи, которые будет выполнять система безопасности. Чем сложнее задачи, тем больше компонентов должно быть в системе безопасности.

Обеспечение безопасности любого объекта заключается в реализации 3-х основных этапов:

- **ОПРЕДЕЛЕНИЕ И ОЦЕНКА ПОТЕНЦИАЛЬНЫХ УГРОЗ**
- **РАЗРАБОТКА МЕР РЕАГИРОВАНИЯ НА УГРОЗЫ**
- **РЕАЛИЗАЦИЯ МЕР ЗАЩИТЫ**

Первые два этапа - это организационные меры, они не требуют больших материальных затрат, но их эффективность подтверждается многолетней практикой (хотя часто и недооценивается потенциальными жертвами).

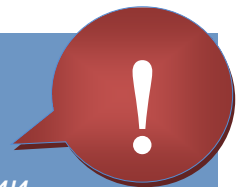
Первая из организационных мер, которую в разной степени выполняет каждый - оценка возможной угрозы. Оценка возможной угрозы проводится на основании объективных и субъективных факторов, с учетом территориального расположения, криминогенной обстановки в районе, рода Ваших занятий, контактов.

Возможный ущерб определяется наличием ценностей (материальных, информационных и др.).

На втором этапе необходимо определить наиболее слабые места, с точки зрения несанкционированного проникновения на объект, и меры защиты, которые Вы можете предпринять.

Меры по защите предусматривают:

- *создание на пути нарушителя физических препятствий;*
- *контроль доступа в помещения;*
- *видеодокументирование;*
- *передачу сигналов тревоги или сообщений о происшествии.*



Создание на пути нарушителя физических препятствий в виде заборов, стальных дверей с секретными замками и решеток на окнах не вызывает больших проблем.

Нам бы хотелось поговорить об остальных пунктах, технических мерах защиты, которые реализуются всевозможными системами безопасности.

Здесь возможны различные варианты в зависимости от выбранных Вами мер по пресечению действий злоумышленника.

Можно установить систему безопасности и подключить ее на пультовую охрану с реагированием вневедомственной охраны или сотрудников МВД. Тогда, в случае тревоги, сигнал поступает в центр пультовой охраны, диспетчер вызывает сотрудников МВД, или вневедомственную охрану (ВО), или частное охранное предприятие (ЧОП), в зависимости от специализации пульта охраны.

Можно установить систему, которая будет лишь посылать уведомление в виде SMS-сообщений на заранее запрограммированный телефонный номер.

В первом и втором случае состав оборудования системы будет примерно одинаковым, отличие только в центральном блоке (контрольной панели).

ЧТО КОНТРОЛИРОВАТЬ?

Целесообразно контролировать:

- **перемещения по прилегающей территории;**
- **проникновение во внутренние помещения;**
- **перемещения в помещениях.**

Перемещения по прилегающей территории можно контролировать с помощью систем видеонаблюдения.

В качестве средств ограничения и контроля доступа уместно использовать аудио и видеодомофоны, телевизионное наблюдение. Это оборудование позволяет принять решение о допуске посетителей без вступления с ними в непосредственный контакт, а также дает возможность оценить обстановку во входной зоне.

Проникновение во внутренние помещения и перемещения внутри контролируются с помощью всевозможных извещателей, которые являются частью охранной сигнализации.

Функционирование извещателей основано на различных физических принципах, а схемотехника позволяет создавать различные по уровню сложности решения - от простых контактных до сложных, использующих цифровую микропроцессорную обработку сигналов и адаптирующихся к внешним условиям.

По дизайну и конструкции извещатели практичны и эргономичны: многие из них можно устанавливать скрытно, а в случае открытой установки такое оборудование не портит своим внешним видом интерьеры внутренних помещений.

ТИПЫ ДАТЧИКОВ

Для оборудования используются различные типы извещателей:

- контактные
(концевые выключатели, кнопки, герметичные магнитные контакты - герконы);
- обрывные;
- вибрационные;
- виброметрические;
- емкостные;
- ультразвуковые;
- оптикоэлектронные
(пассивные инфракрасные, активные инфракрасные);
- микроволновые;
- комбинированные;
- радиоволновые;
- микрофонные и другие.



ЗАЩИТА ОКОН И ДВЕРЕЙ

Для обнаружения нарушения периферии объекта также используют различные извещатели. Окна и двери защищают контактными извещателями, обычно герконами, которые показывают положение форточек, дверных и оконных створок. Дополнительно часто применяют емкостные извещатели, например, мобильные, устанавливаемые на ручки дверей или окон. Для защиты окон и дверей используются так же оптикоэлектронные извещатели (пассивные ИК "шторы", активные ИК барьеры),

извещатели разбития стекла. Для защиты дверей и стен от пролома устанавливают вибрационные, сейсмические и микрофонные извещатели.

ЗАЩИТА ВНУТРЕННИХ ПОМЕЩЕНИЙ

Следующим рубежом охраны является защита объема внутренних помещений. Для того чтобы обеспечить такую защиту применяют так называемые объемные извещатели, или детекторы движения (пассивные ИК и комбинированные, ультразвуковые и др.), ИК барьеры и прочие. На российском рынке услуг безопасности широко представлены как зарубежные, так и отечественные производители оборудования охранных систем: "Alarmcom", "C&K Systems", "Optex", "Ademco", "Scantronic", "Protech", "Visonic", "Полисервис", "Риэлта", "Аргус-спектр" и другие.

Охранные извещатели подключаются к контрольной панели, на которую от них поступает сигнал о состоянии охранных зон (норма или нарушение). Охранные панели позволяют ставить на охрану и снимать с охраны, как отдельные охранные зоны, так и объект в целом.



Существуют программируемые и непрограммируемые панели, без устройств автодозвона или с такими устройствами. Последние наиболее интересны, т.к. позволяют передать тревожное голосовое или sms-сообщение по заранее запрограммированному номеру телефона.

В некоторых случаях при выборе системы безопасности предпочтительнее установить беспроводную сигнализацию. Современные беспроводные сигнализации, во многом превосходят проводные, если речь идет о небольшом количестве датчиков (до 25шт).

Основные преимущества беспроводных сигнализаций:

- не портят интерьер, так как не соединяются проводами с центральным оборудованием;
- нет физического канала связи, а, значит, не может быть обрыва проводов и т.п.

Однако стоит учитывать, что связь с датчиком по радиоканалу может быть прервана, поэтому необходимо выбирать систему, которая самостоятельно может найти датчик.



Как уже отмечалось, систему безопасности можно укомплектовать системой видеонаблюдения.

ВИДЕОНАБЛЮДЕНИЕ

Основными задачами системы видеонаблюдения являются:

- **дистанционный видеомониторинг;**
- **видеодокументирование.**

Дистанционный видеомониторинг позволяет осуществлять проверку целостности прилегающей территории и объектов на ней, периметра объекта, а также контроль перемещений и действия людей внутри помещений.

На мониторе можно просмотреть передаваемое изображения со всех видеокамер, которые входят в данную систему. Выбор изображения с той или иной видеокамеры осуществляется посредством пульта управления.

Видеодокументирование позволяет восстановить ход событий. Найти и опознать нарушителя значительно проще, если есть видео или фотодокументы этих событий.

Основными компонентами для организации телевизионного наблюдения являются:

- **телевизионные камеры**
- **объективы**
- **мониторы**
- **квадраторы (мультиплексоры)**
- **видеорегистраторы**



В современных системах видеонаблюдения используют цифровые видеорегистраторы, их можно сравнить с видео магнитофоном, но при этом запись осуществляется на жесткий диск или флэш-карту, может быть несколько входов для подключения видеокамер и микрофонов и выход для подключения монитора. Многие модели цифровых видеорегистраторов подключаются к сети Интернет для обеспечения удаленного просмотра видеоданных.

Последние годы все доступнее становится оборудование IP видеонаблюдения. IP камера это сервер с потоком текущего видео и звука, и если набрать адрес камеры и ввести пароль, можно просматривать картинку и слышать звук на объекте в режиме реального времени. Камера подключается к Интернету с помощью локальной сети передачи данных, при этом достойное качество можно получить при наличии на объекте выделенной линии.



Охрана объекта с применением современных технологий, например, при сочетании системы видеонаблюдения с выходом в Интернет и с GSM сигнализацией, имеет свое преимущество.

В случае проникновения злоумышленников на объект срабатывает gsm сигнализация, которая отправляет тревожное сообщение на мобильные телефоны. Получив тревожное сообщение от gsm сигнализации, Вы из любой точки мира, через Интернет, обращаетесь к системе видеонаблюдения, оцениваете степень угрозы и вызываете сотрудников МВД. Причем все это без абонентской платы.

Мы советуем устанавливать современные цифровые системы видеонаблюдения. Это не дешево, но оправдано: средства, вложенные в качественную полифункциональную систему видеонаблюдения сегодня, сэкономят более существенные затраты в будущем.



Современная качественная система видеонаблюдения предполагает следующее оборудование:

- **цифровой видеорегистратор** (качественный видеорегистратор стоит от 15000 до 25000 руб.);
- **видеокамеры** (1 видеокамера хорошего качества стоит от 2500 до 5600 руб.);
- **бесперебойный блок питания** (3000-7000 руб);
- **кабели и прочие расходные материалы** (5000-10000 руб.).

Конкретный состав оборудования зависит от количества камер, условий их работы (вне или внутри помещений), расстояний между телекамерой и монитором (постом наблюдения) и прочего. Разнообразие конструкций, технических характеристик и дизайна камер позволяет выбрать наиболее подходящую для каждого конкретного случая использования.

В КАЧЕСТВЕ ЗАКЛЮЧЕНИЯ

Система охранной сигнализации осуществляет контроль движения на объекте, открытия дверей, ворот, целостности окон, стен, решеток и т.д.

Все системы могут быть объединены в комплексную систему безопасности, в том числе с применением компьютерных сетей и возможностью удаленного доступа (просмотр изображения с видеокамер, управление, конфигурирование), а также записи видеоинформации и протоколирования событий в системе контроля доступа и охраны. Система бесперебойного питания и резервных аккумуляторов обеспечивает работоспособность всех сигнализационных, видео, контрольных и компьютерных систем при пропадании напряжения в электрической сети.