
А.П.Кашкаров
Справочное пособие
по СИСТЕМАМ ОХРАНЫ
с ПИРОЭЛЕКТРИЧЕСКИМИ
ДАТЧИКАМИ

2016

«Справочное пособие по системам охраны с пироэлектрическими датчиками. / Кашкаров А.П.»: ИП РадиоСофт; Москва; 2016
ISBN 978-5-93037-310-3

Аннотация

Справочное пособие будет полезно разработчикам и установщикам популярных (современных) охранных систем с пироэлектрическими детекторами. В книге приведены сравнительные характеристики разных систем и модификаций, а также даны рекомендации по совместимости разных датчиков– пироэлектрических сенсоров с контрольными панелями систем охраны разных производителей.

Проблема «нейтрализации» охранных сигнализаций, установленных стационарно, не теряет свой остроты: страховые выплаты хоть и покрывают ущерб в случаях потери имущества после несанкционированного проникновения в охраняемые электроникой помещения, однако заинтересованную общественность беспокоит то, чтобы в будущем не участились подобные случаи. Однако, сегодня охранные системы с датчиками движения популярны не только на производстве, но и в «частном секторе»: с их помощью граждане охраняют городскую и загородную недвижимость, автомобили, вещи и оборудование.

В книге отражен предметный разбор и проблематика случаев несанкционированного проникновения, которые происходили при отсутствии срабатывания сигнализации, то есть в результате блокирования электронной системы, «защищенной» пироэлектрическими детекторами. Даны принципы действия современных пироэлектрических детекторов, для понимания и определения стратегии их лучшей защиты и устранения критичных факторов уязвимости систем охраны.

Для специалистов, разработчиков и широкого круга читателей, практикующих защиту своего имущества и заинтересованных в безупречной работе своих охранных систем.

Андрей Кашкаров
Справочное пособие по системам охраны с пироэлектрическими датчиками

От автора

Прочтите книгу! Несложными и проверенными на практике способами удается полностью нейтрализовать современную охранную систему на основе промышленных и широко распространенных во всех странах мира (для охраны квартир и производственных помещений) датчиков движения – пироэлектрических детекторов. Производители охранных систем, разумеется, знают о недостатках своих датчиков, но они никогда и не гарантировали их 100 % работоспособность (защиту охраняемых помещений) в любых условиях. Кроме того, многое зависит и от возможностей, мотивации и способов, которыми смонтирована система.

Сегодня пришло время заявить о проблеме с датчиками движения громко. В обосновании приведенного вывода в материалах Приложения показана суть практических экспериментов, послуживших практической основой материала данной книги. Пользуйтесь и процветайте!

Андрей КАШКАРОВ

Глава 1
Современные модули и датчики систем охранных сигнализаций

Ценность профессионала заключается в том, что он может предложить услуги по монтажу сигнализации по проекту любой сложности на различных объектах. Большой опыт проектирования и монтажа систем охранно-пожарной сигнализации, позволяет совершенствовать навыки и работать с оборудованием различных производителей, а это большой плюс сегодня в решении нестандартных задач. Итак, каждый отдельный объект требует индивидуального подхода в соответствии с уникальной конфигурацией системы охранной сигнализации, которая подходит для дома, квартиры или дачи. Отсюда наиболее эффективным решением для обеспечения сохранности личного имущества является установка системы охранной сигнализации в квартиру, дом, дачу, на передвижном объекте (автотранспорт) т. д.

1.1. Типы сигнализаций

Рынок электронного оборудования охранно-пожарной сигнализации предлагает широкий выбор устройств, позволяющих построить систему и осуществить монтаж сигнализации загородного дома или квартиры любого уровня сложности

По типу оповещения системы охранной сигнализации в квартиру или дом можно условно разделить на автономную сигнализацию, GSM-сигнализацию и систему охранной сигнализации, подключенной на пульт централизованного наблюдения (далее: пультовая охрана). Также возможны и сочетания (комплекс) элементов различных сигнализаций в едином электронном блоке, что, несомненно, повышает его надежность. Рассмотрим эти варианты (элементы единого комплекса) по существу, ведь принцип работы у всех них различен.

Автономная сигнализация реагирует на тревожное событие включением звуковых, световых или светозвуковых оповещателей (сирены, строб-вспышки, маяки и т. п.).

GSM сигнализация, кроме способов оповещения, присущих автономной сигнализации, может отправлять голосовые и текстовые сообщения на сотовый телефон хозяина (установщика) охранной системы посредством встроенного GSM-модуля. В структурах охраны «хозяином», или ответственным лицом, принято называть «хоз-органа» – этими определениями мы будем пользоваться и далее в книге. При этом важно понимать, что GSM сигнализация с функцией информирования не ведет к значительному увеличению сметной стоимости системы, но серьезно расширяет функциональные возможности системы сигнализации.

На рис. 1.1 представлена блок-схема центрального пульта охраны и других ее составляющих.

Охранная система (исполнение, особенности подключения) может быть изготовлена в двух исполнениях: беспроводной и проводной. Принцип взаимодействия модуля и элементов системы в данном случае один и тот же.

Плюсы и минусы беспроводной охранной сигнализации

На большинстве объектов устанавливается традиционная система проводной охранной сигнализации, но существует и альтернатива.

Преимуществом беспроводной охранной сигнализации является то, что при монтаже такой системы не требуется штробление стен, перекрытий или укладка кабель-каналов. Беспроводные системы выбирают в тех случаях, когда установка сигнализации производится после чистовой отделки и прокладка проводов в помещениях невозможна из-за соображений эстетики.

Рис. 1.1. Блок-схема центрального пульта охраны и других ее составляющих

К недостаткам беспроводных систем относится необходимость замены элементов питания в датчиках, приборах и сиренах. Когда на объекте этих элементов достаточно большое количество, то это занимает большое количество времени, что увеличивает затраты на техобслуживание. Второй недостаток – это ограниченность в применении беспроводных систем. Радиоканальная система охранной сигнализации может давать сбои в зданиях с массивными перекрытиями или с повышенными источниками электромагнитного излучения. Однако как компромиссный вариант, возможна установка комбинированной охранной системы, в которой есть участки с проводной и беспроводной связью.

У проводных систем охраны также имеются свои недостатки, о которых будет не лишним упомянуть. Первый и, пожалуй, самый главный недостаток – это высокая сложность монтажа. Связано это с тем, что при установке данной охранной системы возникает необходимость прокладывать линии связи. Помимо этого, большое количество проводов могут испортить дизайн помещения. Но эти недостатки легко устранить при помощи правильного качественного монтажа.

Проводная сигнализация, несмотря на свой «возраст» (относительно времени разработки), по сей день является самым надежным видом защиты от несанкционированного проникновения на объект. Грамотно выполненный профессиональными мастерами монтаж данной охранной системы поможет сделать дом, офис или другой объект неприступной крепостью.

Существуют юридические (правовые) особенности.

Внимание, важно!

Стараясь обезопасить свой бизнес, жизнь, дом путем установки систем скрытого видеонаблюдения и шпионских видеокамер соблюдайте законы Российской Федерации.

Конституция Российской Федерации: статья 24 1. Сбор, хранение, использование и

распространение информации о частной жизни лица без его согласия не допускаются.

Уголовный кодекс Российской Федерации (в редакции от 28.12.2004 г.):

• Статья 137. Нарушение неприкосновенности частной жизни.

• Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

Пультовая охрана объектов имеет свои особенности. Система охранной сигнализации, установленная в доме или квартире, находится под постоянным наблюдением операторов пульта централизованного наблюдения (на профессиональном языке это называется ПЦО), что позволяет отделу охраны, в том числе вневедомственной охраны в системе МВД, или муниципальной полиции реагировать на тревожные события на объекте.

1.2. Главные различия в способах монтажа

Сигнализацию на объектах по способу монтажа можно разделить на проводную и беспроводную системы. Проводная система охраной сигнализации требует прокладки кабеля ко всем устройствам, входящим в ее состав: датчикам сигнализации, сиренам, пультам управления и т. д.

Беспроводная сигнализация проста в монтаже и эксплуатации, легко наращивается без дополнительной прокладки кабеля к устройствам системы. Все устройства (датчики сигнализации, пульты управления, сирены, маяки) подключаются к системе беспроводной охранной сигнализации по радиоканалу. К преимуществам беспроводной сигнализации можно отнести и то, что при перестановке мебели или ремонте в офисе (квартире, дачном доме) все беспроводные датчики и пульты управления легко демонтируются и перемещаются на новое место.

К недостаткам беспроводной сигнализации можно отнести регулярную замену источников питания (элементы, батареи, аккумуляторы) в беспроводных датчиках и пультах управления. Как правило, такая замена производится 1–2 раза в год, но корпус брелоков и датчиков системы все равно нужно вскрывать – таковы нюансы регламентного обслуживания системы.

По сути, беспроводная система намного более уязвима для несанкционированной блокировки, чем система с датчиками и пультами, соединенными кабелем, во многом поэтому беспроводные системы, несмотря на их кажущуюся внешнюю привлекательность или простоту в установке, среди профессионалов считаются любительскими, непрофессиональными. Одним из простых способов злоумышленники пользуются до сих пор: дистанционное (за несколько метров и десятков метров) блокирование радиоканала посредством переносных и весьма компактных устройств-«глушилок» делает всю дорогостоящую беспроводную систему охраны бесполезной.

На рис. 1.2 представлен внешний вид электронного устройства А-100, которое блокирует по радиоканалу сигнализации в частотных диапазонах 900/1800 МГц (сотовая связь); 2,4 ГГц (Wi-Fi) и других. О более существенных недостатках беспроводной системы охраны мы подробно поговорим далее, в специальном разделе.

Рис. 1.2. Электронное устройство-«глушилка» по радиоканалу

Устройство делает невозможным сотовую связь (и Wi-Fi) в зоне своего действия – в радиусе 30 метров, то есть им можно блокировать беспроводные датчики охранной системы из соседнего помещения. Современная беспроводная охранная система, конечно же, имеет функцию постоянного контроля связи по радиоканалу между удаленными датчиками и центральным блоком (модулем), и вырабатывает сигнал «тревоги».

Однако даже если предполагать, что охрана (группа быстрого реагирования) после такого сообщения электронного устройства может «усилить бдительность» и направить на объект пристальное внимание, пытаться переустановить сигнализацию в режим «охрана», то это все равно не отменяет бесполезности (блокировки) действия многофункциональной электронной системы охраны с беспроводным способом связи между пультом и удаленными датчиками (PIR-сенсорами) в случае применения относительно простой и вполне доступной «глушилки». Приобрести сегодня такое устройство по цене всего 10 000 рублей не составляет труда.

Кроме того, для нахождения «шпионской и глушительной» техники в контролируемом ДД помещении обратите внимание и на другие устройства.

К примеру, на миниатюрный универсальный детектор видеокамер и радиожучков ХВ-68, который функционально сочетает в себе два устройства – прибор для оптического обнаружения скрытых видеокамер и детектор подслушивающих устройств.

Обнаружитель скрытых камер использует в своей работе физическое явление отражения света от линзы объектива. Вокруг окна для поиска бликов расположены сверхъяркие светодиоды, испускающие направленный свет, который отражаясь от линзы объектива становится видимым бликом. Частота мигания подсветки регулируется. Детектор «жучков» улавливает сигнал от «жучков» (радиозакладок) и оповещает владельца о местонахождении подслушивающего устройства. Встроенный частотомер обнаружит любые беспроводные подслушивающие устройства, включая сотовые телефоны, приборы, передающие информацию по Bluetooth, беспроводные видеокамеры, радиомикрофоны и т. д. Имея миниатюрные размеры и вес и такие функциональные возможности детектор скрытых видеокамер и «жучков» может находиться постоянно на важных деловых переговорах.

А имеющаяся возможность подключения наушников, поставляемых вместе с детектором прослушки, делает его работу бесшумной и соответственно незаметной для посторонних. Имеется вибросигнал.

Эксплуатация нужного нам в части обнаружения «глушилок» детектора поля имеет особенности. А устройства – два режима работы: виброрежим и акустический режим. Для включения нужного режима вытяните антенну, установите переключатель справа в нужное положение – динамик (акустический режим), зачеркнутый динамик (виброрежим), off – выключение устройства. Далее крутите колесо настройки чувствительности «sensitivity» для настройки чувствительности.

Настройка осуществляется таким образом: поднесите детектор к сотовому телефону в момент осуществления звонка, индикаторы начнут мигать.

Кроме того, и охранно-пожарные сигнализации наряду с охранными функциями могут контролировать помещения на предмет возгорания или задымления. Для этого система дополняется пожарными датчиками, которые в зависимости от типа монтажа охранной сигнализации также могут быть беспроводными и проводными.

Что касается частного случая – охранной сигнализации для квартиры, дачи, офиса или загородного дома, то предполагается, что она защитит дом от воров. При обнаружении злоумышленника система включит сирену, отправит сигнал на ваш мобильный телефон (СМС или звонок) или вызовет группу реагирования (охрану). Но всю рекламную информацию, красочно расписанную в буклетах, анонсах и упаковках электронных устройств рассматриваемого назначения надо, что называется, «делить на 10».

Важно и другое. Почти любая система имеет блок резервного питания с аккумуляторной батареей, который позволит системе работать в течение некоторого времени при отключении централизованного электропитания.

Почти любая современная система охраны универсальна и может быть дополнена датчиками дыма или газа. Таким образом, почти любую современную систему охраны можно расширить дополнительными датчиками: движения (внутренними и уличными), открытия двери, разбития стекла, утечки газа.

Если вернуться к схеме, представленной на рис. 1.1, то очевидно, что комплект оборудования включает в себя несколько составляющих, в том числе контрольную панель, блок резервного питания с аккумулятором, сирену, датчик(и) открытия двери, датчик(и) присутствия, в беспроводных системах – два (и более) брелока, в проводных системах – до 100 метров резервного кабеля.

Почти для любой системы, помимо стандартных, могут быть реализованы различные способы постановки на охрану и снятия с охраны: поднесение ключа (или бесконтактного брелока) к считывателю, нажатие кнопки на брелоке (как автомобильная сигнализация), набирание кода на клавиатуре.

Как сказано выше, беспроводная система подразумевает отсутствие кабелей между датчиками и контрольной панелью, это упрощает установку и не вредит возможному изменению конфигурации и косметическому ремонту помещения. Проводная система более надежна и не требует периодической замены элементов питания в датчиках, но для нее необходимо скрытно (в штробах – предварительно сделанных монтажником по стенам помещения) прокладывать кабель и (или) защищать его кабель-каналом.

Важнейшее значение имеет квалификация монтажника системы. Важно сделать подключение проводами между датчиками и центральным блоком нешаблонно. Речь идет о том, что не обязательно красный провод должен быть подключен к «+» питания системы, а провод черного цвета – к «—». Такие маленькие хитрости усложнят антисоциальным элементам (даже подготовленным и предварительно натренированным на аналогичном типе электронных устройств) доступ к блокировке системы охраны. Об этом мы также поговорим в соответствующем разделе в книге.

Таблица 1.1

Отличия между проводными и беспроводными современными системами охраны

Тип системы	Самая простая	GSM проводная	GSM беспроводная	Профессиональная проводная	Профессиональная беспроводная
Стоимость комплекта оборудования	4540 рублей	10 160 рублей	7710 рублей	15 800 рублей	23 040 рублей
Провода до датчиков	Да	Да	Нет (можно подключить также и проводные датчики)	Да	Нет (можно подключить также и проводные датчики)
Способы реагирования	Сирена	Сирена, звонок на телефон (до 3 номеров), СМС на телефон (до 3 номеров)	Сирена, звонок на телефон (до 4 номеров), СМС на телефон (до 4 номеров)	Сирена, СМС на телефон (до 10 номеров), сигнал на пульт охраны ЧОП	Сирена, СМС на телефон (до 10 номеров), сигнал на пульт охраны ЧОП
Сложность самостоятельной установки	Просто	Просто	Очень просто	Сложно (требуются специальные знания и программное обеспечение)	Сложно (требуются специальные знания и программное обеспечение)
Частота замены батареек в датчиках	Не нужно	Не нужно	8 месяцев — 1 год (в зависимости от температуры хранения). Батарейки стандартные (Крона)	3 года (батарейки специальные)	3 года (батарейки специальные)

Тип подключения датчиков	4-жильный кабель (или витая пара)	4-жильный кабель (или витая пара)	Радиоканал до 200 метров (частота 433 ГГц)	Радиоканал до 400 метров (частота 668 ГГц)	Радиоканал до 400 метров (частота 668 ГГц)
Стандартный способ постановки на охрану	Ключ-таблетка	Ключ-таблетка, управляющее СМС, звонок с телефона	Брелок, управляющее СМС, звонок с телефона	Кодовая клавиатура	Кодовая клавиатура, брелок
Стандартное время работы основного блока от аккумуляторов	24 часа	48 часов	6 часов	24 часа	24 часа
Абонентская плата	Не требуется	1 рубль за отправленное СМС (в зависимости от тарифа оператора)	1 рубль за отправленное СМС (в зависимости от тарифа оператора)	1 рубль за отправленное СМС (в зависимости от тарифа оператора). При заключении договора с ЧОП — от 700 рублей в месяц)	1 рубль за отправленное СМС (в зависимости от тарифа оператора). При заключении договора с ЧОП — от 700 рублей в месяц)

В табл. 1.1 представлены наиболее существенные отличия между проводными и беспроводными современными системами охраны.

1.3. Виды датчиков движения для охранных сигнализаций

Установка охранной сигнализации является одним из самых простых и легких способов защиты помещений от несанкционированного проникновения. Свободный рынок электронных устройств предлагает большой выбор систем сигнализации, наиболее подходящих для охраны конкретного объекта. Главным элементом охранной сигнализации является пироэлектрический датчик движения. Такое устройство предназначено для контроля определенной области и подачи сигнала при обнаружении двигающегося человека.

1.3.1. Устройство датчика движения

По способу крепления и подключения различают настенные и накладные, проводные и беспроводные, внешние и внутренние датчики движения (далее – ДД) охранной сигнализации. Некоторые модели подобных систем имеют иммунитет от домашних животных, то есть устройство не срабатывает на движение объекта, масса которого меньше 25 кг.

Принципы работы и применение ДД

Среди разработок не ранее 2010 года известны несколько видов детекторов перемещений, они имеют специфические отличия по типу примененных датчиков.

Ниже будут описаны детекторы перемещения на основе датчиков инфракрасного (ИК) излучения.

ИК излучение находится в электромагнитном спектре. Длина волны больше длины волны видимого света. ИК излучение невозможно увидеть, но оно характерно фиксируется при помощи специально предназначенных для этого датчика. Человеческое тело, впрочем, как и у животных, довольно интенсивно излучает в ИК диапазоне. Максимум такого излучения преобладает в длине волны 9,4 мкм. Распознавание ИК излучения основывается на пироэлектрических датчиках. Они сделаны из специального кристаллического материала, который при воздействии на него ИК излучения вырабатывает поверхностный электрический заряд. Встроенный в датчик усилитель на полевом транзисторе значительно повышает распознавание этого заряда и обеспечивает формирование управляющего напряжения. Поскольку датчик срабатывает на ИК излучение в широком диапазоне, для

сужения последнего используется фильтр специального назначения, ограничивающий восприятие датчиком ИК излучения только в диапазоне от 8 до 14 мкм.

В электрической схеме детектора перемещений (многократно описанной в литературе, в т. ч. автором, рис. 1.3) используется дешевый счетверенный операционный усилитель LM324. Первые два ОУ – IC1A, IC1B – выполняют функции усилителя, два другие – функци ИК компаратора. Выпрямленный диодами D3, D4 сигнал поступает на одновибратор IC2, который управляет транзисторным ключом Q1. В цепь коллектора транзистора Q1 включена обмотка исполнительного реле.

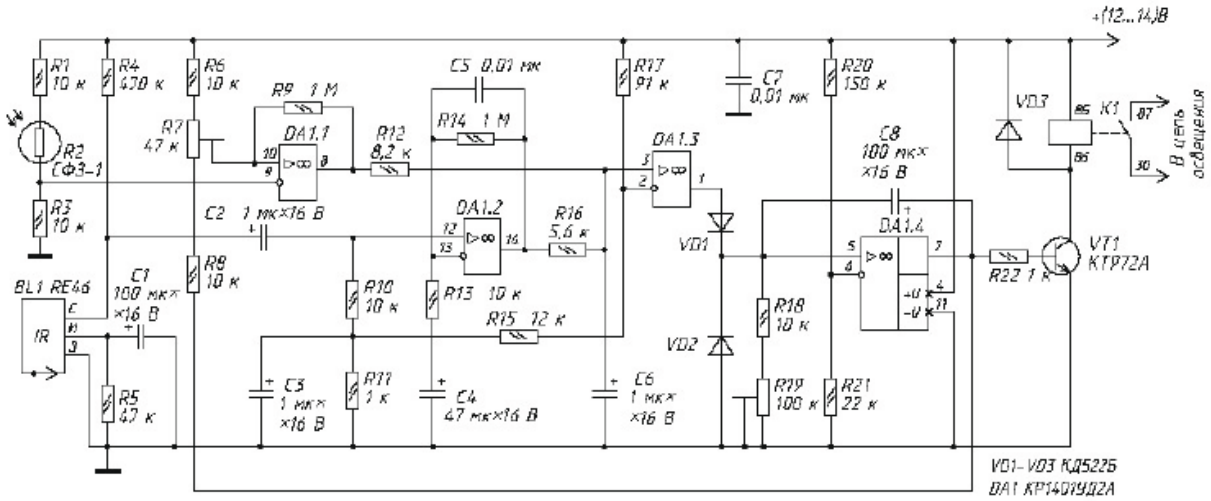

Рис. 1.3. Электрическая схема детектора перемещения

Не всегда удобно или возможно привязать датчик с исполнительным устройством посредством проводов. В таких случаях оптимальной является связь датчика с исполнительным устройством по радиоканалу. В странах Европы и США разрешена работа устройств дистанционного управления и автосигнализаций на частоте 418 МГц. Устройства, отвечающие условиям применения для работы на этой частоте, не требуют сертификации и разрешения. Если раньше существовали некоторые трудности в проектировании и изготовлении таких приемопередающих устройств, то после выпуска унифицированных модулей передатчика TM1V и приемника RM1V проблема реализации связи устройств дистанционного управления по радиоканалу на частоте 418 МГц попросту исчезла.

Совместимость работы близкорасположенных устройств ДУ обеспечивается благодаря использованию микросхем кодера в передатчике и декодера в приемнике. При перемещении человека в зоне действия ИК датчика на выводе *1* IC1B возникает положительный перепад напряжения, который через диод D2 поступает на вывод *6* IC2A, и в результате его потенциал становится выше потенциала на выводе *5* . На выводе *8* IC2A формируется высокий уровень. Затем по второму сигналу с датчика на выводе *1* IC1B формируется отрицательный перепад. Это в свою очередь приводит к снижению потенциала на выводе *5* IC2A, что также формирует напряжение высокого уровня на выводе *8* IC2A. Положительный перепад напряжения на выводе *8* IC2A через конденсатор C6 поступает на IC2B. В результате на ее выходе (вывод *1*) формируется низкий уровень. Этот уровень через диод D3 прикладывается к выводу *5* IC2A и переключает состояние этой микросхемы на время разряда конденсатора C6 через резистор R17 или R18.

Таким образом, сигнал от детектора перемещений принимает модуль приемного устройства, в который входит собственно модуль приемника RM1V, связанный с декодером HT694 фирмы Holtek, программируемым переключателем SA для работы с определенным передатчиком. Декодер последовательно получает три группы битов, содержащих данные и адресную информацию, хранит их, а затем сравнивает их. При совпадении двух из них, декодированные данные появляются на одном из выводов – *1, 2, 3* или *4* – в зависимости от

того, какой переключатель выбора номера передатчика включен. Затем управляющий сигнал высокого уровня поступает на четырехэлементную схему-защелку IC3.

На выводе *5* IC1 при приеме верных данных всегда формируется сигнал логической 1, который открывает транзистор и запускает таймер IC2, формирующий на выводе *3* (выход Momentary) сигнал длительностью около 2 с. Этот сигнал используется для управления зуммером, служащим для индикации работы передатчика.

В приведенной на рис. 1.6 схеме используются выходы на полевых транзисторах с рабочим током стока около 150 мА, что достаточно для подключения светодиодных индикаторов. Имеется возможность сброса в нулевое состояние микросхемы IC3. Для этого следует кратковременно соединить вывод Reset с выводом источника питания +5 В. Обычно первичным источником питания для такой схемы служит сетевой адаптер на напряжение 12 В.

Датчики движения условно принято делить на четыре типа: микроволновые ДД, сигнализирующие об изменениях отражения излучаемых электромагнитных волн, проводные. Далее рассмотрим их функционал и принципиальные отличия.

1.3.2. Примеры и особенности пироэлектрических детекторов

Микроволновый датчик движения модификации Pyronix EQUINOXE

Микроволновые датчики, сигнализирующие об изменениях отражения излучаемых электромагнитных волн. Принцип работы таких устройств основан на эффекте Доплера – как только в контролируемой зоне появится движущийся токопроводящий объект, сигнализация сработает. Важным преимуществом микроволнового датчика является способность обнаружения движения за тонкими гипсовыми, деревянными и стеклянными перегородками. Подобные устройства обладают высокой точностью, реагируя даже на незначительные движения с малой скоростью. Именно они широко используются в современных системах охраны и безопасности.

Внешний вид проводного датчика движения модификации Pyronix Colt XS (производство Англия) представлен на рис. 1.4. Внешний вид проводного датчика движения модели Pyronix Colt10DL (производство Англия) представлен на рис. 1.5.

На рис. 1.6 и 1.5 представлены проводные датчики к охранным системам известных моделей Sapsan и Mega SX. Датчик движения проводной Pyronix Colt10DL предназначен для установки внутри помещения. Его особенность – невосприимчив к животным до 10 кг. Внешний вид датчика движения проводной PyronixColtQuadPI (производства Англия) представлен на рис. 1.6. Датчик движения проводной Pyronix Colt Quad PI (Англия) предназначен для установки внутри помещения. Невосприимчивый к животным до 20 кг.

Датчик движения проводной DSC LC-151 (производства Канада) представлен на рис. 1.7. Датчик движения проводной DSC LC-151 предназначен для уличной установки. На рис. 1.8 представлен внешний вид проводного датчика движения Pyronix XD10TTAM (производства Англия). Датчик движения проводной Pyronix XD10TTAM предназначен для уличной установки.

1.3.3. Принцип работы PIR-сенсоров

Микроволновые инфракрасные датчики движения охранной сигнализации на примере DSC LC-101CAM обнаруживают перемещающиеся объекты за счет выявления изменения теплового излучения. Движущееся тело выделяет тепло, что регистрируется чувствительным сенсором, расположенным за сегментированными зеркалами аппарата. Охранную систему, работающую на основе инфракрасного излучения, можно использовать в помещениях и на открытых площадках, поскольку такой датчик учитывает только собственную температуру объектов. Кроме того, этот датчик не излучает никаких сигналов, работая только в качестве приемника сигнала, что говорит о высоком уровне безопасности его эксплуатации.

Рис. 1.4. Pyronix Colt XS

Рис. 1.5. Pyronix ColtlODL

Рис. 1.6. PyronixColtQuadPI (производства Англия)

Рис. 1.7. DSC LC-151

Рис. 1.8. Pyronix XD10TTAM

Ультразвуковые датчики выявляют движение в результате сканирования пространства ультразвуковыми волнами. Такое устройство оснащено генератором звуковых волн, которые отражаются от окружающих объектов и поступают в приемник. Сигнал об обнаружении движения фиксируется после регистрации изменения излучаемых и принимаемых волн. Ультразвуковой датчик движения охранной сигнализации желательно устанавливать в помещениях сложных конфигураций, поскольку именно при помощи такого устройства удастся полноценно контролировать «слепые» зоны.

Рассмотренные датчики эффективно работают в составе охранной системы вместе с цифровыми комбинированными извещателями 1ИК и 2ИК с передачей сигналов тревоги по СВЧ-каналу. Такие извещатели имеют и функцию антимаскирования.

Комбинированные датчики на примере DSC LC-104PIMW сочетают в себе несколько технологий обнаружения. Купить комбинированный датчик движения для охранной сигнализации, значит, обеспечить высокий уровень безопасности любого объекта. В устройстве DSC LC-104PIMW (ценовой диапазон по состоянию на июль 2015 года – от 1000 руб. и выше) для обнаружения движущихся объектов используется инфракрасный сенсор и микроволновой детектор Doppler. Устройство, предлагаемое канадским производителем, дополнительно оснащено защитой от скачков напряжения.

1.3.4. Область применения датчиков движения

Чаще всего ДД используются в системах, предназначенных для охраны жилых домов, квартир, офисов, студий. При помощи таких устройств можно эффективно выявлять нарушителей, проникших в помещение банка, магазина или склада.

Рис. 1.9. Внешний вид популярных сегодня датчиков движения

Подобные аппараты необходимы и для защиты автомобиля от угона – при обнаружении малейших движений сигнализация отпугнет злоумышленника и сообщит о произошедшем владельцу транспортного средства. Ассортимент датчиков движения представлен на рис. 1.9.

1.4. Разновидности датчиков движения для охранной сигнализации

Современный рынок охранной техники предлагает датчики движения таких производителей, как «Ajax», «Crow», «LifeSOS», «Страж», «DSC», «Altronics», «SMART SECURITY», «Magnum», «Satel» и др. В разновидностях подобных систем немудрено заблудиться. Датчики «LifeSOS» относятся к средней ценовой категории, а если вы желаете купить более дорогие и мощные устройства, то обратите внимание на модели отечественного бренда «Страж». Тем не менее, эффективность работы устройства будет зависеть не только от исходных параметров, но и от качества монтажа. Об этом мы поговорили выше. При установке электронного устройства важно учитывать много параметров, чтобы обеспечить оптимальную зону контроля, поэтому монтаж датчика движения охранной сигнализации – удел профессионалов.

1.5. Специфика установки и настройки пироэлектрических детекторов в индивидуальных условиях

Монтаж оборудования является не менее важным, чем его правильный выбор. От того

насколько правильно выбрано место для его установки зависит и чувствительность устройства. В системе охраны этим манкировать нельзя и даже опасно. Для охранных датчиков этот параметр будет наибольшим при пересечении человеком зоны контроля под углом. Поэтому, устанавливая устройство, необходимо заранее спрогнозировать, в каких направлениях будет осуществляться движение.

В связи с этим рассмотрим рекомендуемую схему правильного расположения датчика движения.

1.6. Рекомендуемая схема правильного расположения датчика движения

Направление оборудования на источники тепла приведет к ложным срабатываниям.

Высота расположения датчика должна быть не менее 1,5 м, при этом следует избегать попадания прямых солнечных лучей на линзу прибора. Нельзя прикасаться к пироэлектрическому сенсору руками, оставшиеся на зеркале следы уменьшат чувствительность.

Подключение прибора осуществляется через специальные клеммы. Обычно в качестве аккумулятора используются батарейки с напряжением от 9 до 14 В. Положительная и отрицательная клеммы обозначаются плюсом и минусом, что позволяет правильно подключить источник питания.

Настройка прибора выполняется при перемещении платы внутри корпуса. Но существуют устройства лишенные такой возможности. В них настройка контролируемой зоны выполняется следующим образом: часть линзы просто заклеивается бумагой.

После настройки датчика индикатор отключается. Это необходимо для того, чтобы возможный антисоциальный элемент не смог отследить зону контроля.

Технические характеристики

Датчик движения ИК, проводной, типа «штора», для контроля дверей, окон помещения. Негерметичный с двухпроводным типом подключения для внутренней установки.

Питание…….. 12/24 В
Подключение…….. 4-проводное
Совместимость…… охранные системы Magellan, SP, EVO и др. совместимые
Тип датчика…….. проводной, аналоговый, ИК
Тип сенсора…….. один 2-элементный сенсор
Регулируемое положение линзы…….. 0° или 10°
Обнаружение движения руки……. зона 2,1 х 1,5 м для СКД
Обнаружение тела человека……. зона 6 х 4,5 м для систем охраны

Регулируемое время сигнала тревоги. Запатентованный режим автоматического подсчета импульсов. Автоматическая температурная компенсация. Встроенный металлический экран, повышающий помехозащищенность. Датчик вскрытия корпуса.

1.7. Инфракрасный электронный стационарный детектор движения Swan Quad

Сенсорный, с защитой от срабатывания сигнализации на животных, с 4-импульсным пироэлектрическим оповещением и возможностью включения освещения внутри и вне дома, в комплекте без установочного кронштейна. Охранный датчик движения (объема,

присутствия) устанавливается в шлейф ОПС для контроля за периметром в радиусе 18 м. Кроме основной функции обнаружения присутствия (перемещения) теплоизлучающего крупногабаритного объекта, извещатель является коммутатором – включателем/выключателем освещения.

Основное назначение прибора – охрана периметра внутренних помещений офисов и квартир с помощью пультовых и GSM сигнализаций. Дополнительно ДД применяется в качестве реле включения освещения. Настройки квадросенсора позволяют регулировку счетверенного пироэлектрического сенсора, анализируя срабатывание на размеры и температуру движущегося объекта. Стандартные настройки детектора не позволяют передачу тревожного сигнала при обнаружении объекта весом до 25 кг (дети, домашние животные не вызовут автоматического включение света).

1.7.1. Принцип работы

При попадании объекта (размеров и температуры больше заданных в настройке) в инфракрасное поле излучения детектора резко возрастает напряжение на выходе реле. Фокусировка широкоугольной линзы на объекте передаёт многоимпульсные сигналы на контроллер ОПС. Разница посегментного импульсного ИК излучения выдает оповещение о движении и перемене температуры окружающей среды. Нормально замкнутые сухие контакты реле детектора, передающие импульсы, включаются в режим «тревога».

Контроллер GSM, установленный в загородном коттедже, на даче, в гараже, передаст тревожное сообщение по сотовой сигнализации. Клиент может в режиме реального времени получить сигнал датчика и отреагировать. Оповещатель охранной системы подключается к видеорегистратору в помещении и включает удаленную запись событий. Это допустимо: отечественные сигнализации, как правило, снабжены исполнительным блоком с 4—12 выходами реле. Данные контроллеры могут быть заменены комплектами на базе «Сапсан», «Mega», «Страж».

Далее рассмотрим преимущества ИК-детектора.

1.7.2. Преимущества ИК-детектора

Прежде всего – это тамперная защита. Быстрая двунаправленная температурная компенсация по объекту. Комфортный мини-дизайн прибора (впишется и в дом, и в офис). А экономичность – это одна из «бюджетных» проводных ИК моделей на современном рынке охранного оборудования. Отличительные характеристики говорят за себя, поскольку это устройство:

- с иммунитетом к объектам до 25 кг (движение животных),
- 18-метровой зоной реагирования,
- рабочим углом обзора свыше 90°,
- счетверенным квадросенсором пироэлемента (с четырехимпульсной изменяемой шириной),
- жесткой (в противоударном исполнении) линзой G сенсора, микропроцессором SMD с регулировкой чувствительности.

Не обойдена вниманием интеграция в системы охранного видеонаблюдения и автоматического освещения. Как вариант и перспектива (при соответствующем подключении) устройство запускает видеорегистраторы видеонаблюдения, включает светильники уличного и внутреннего освещения.

Технические характеристики устройства SWAN QUAD PIR

Пироэлемент	Quad (счетверенный) PIR
Ток потребления:	
ожидание	8 mA ± 5%
тревога	10 mA ± 5%
Термокомпенсация	есть
Настройка	длина импульса (2–4 ед.)
Время срабатывания	
Начальное время запуска	2 сек ± 0,5 сек 60 сек ± 5 сек
Выход реле (сухой контакт)	Н.З. 28В 0.1А 27 Ом Н.З. 28В 0.1А 10 Ом
Питание	от 8,2 до 16 В
Рабочая частота	868/916,5 МГц
Светодиод	вкл. при сигнале «Тревога»
Рабочая температура	–20 ...+60 °С
RFI Защита	30V/m 10 - 1000 MHz
EMI Защита	50,000 V
Дальность эффективной работы	18 м
Размеры	92×59×37 мм
Вес	40 г

На рис. 1.10 представлена условная схема работы ДД на объекте с указанием чувствительности по зонам доступа. Устройство позволяет выбрать широкий диапазон высоты от 1,8 до 2,4 метра без дополнительной калибровки. Датчик тестируется встроенным в него светодиодом (функция – светодиодный контроль). Возможны настенные, потолочные, угловые варианты установки с кронштейном из комплекта поставки.

Месторасположение выбирается в соответствии с угрозой наиболее вероятного обнаружения взломщика. Важно соблюдать удалённость от источников тепла, прямого солнечного света.

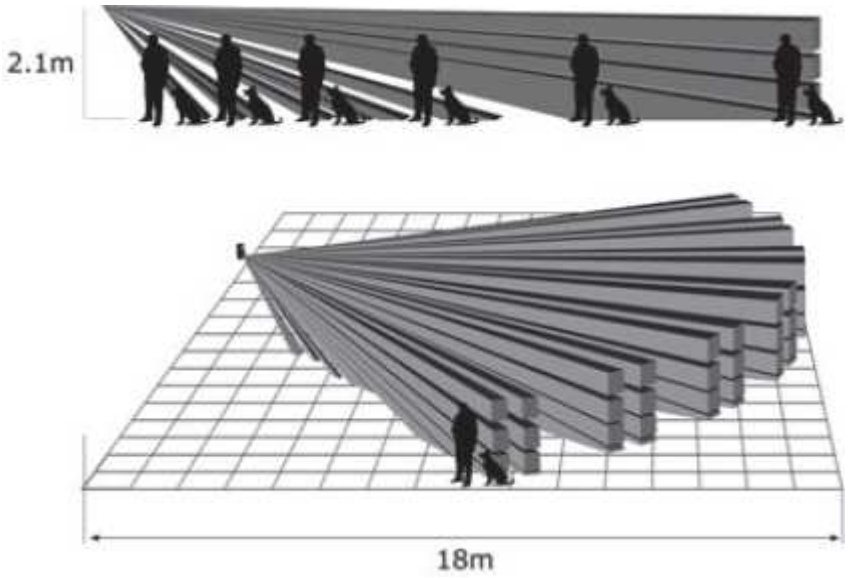

Рис. 1.10. Условная схема работы ДД на объекте с указанием чувствительности по зонам доступа

Датчики движения могут различаться не только по своему оформлению, но и предназначению:

• для энергосберегающего освещения (выключатели светильников, прожекторов, ламп, фонарей, патронов, ночников, кранов, вентиляторов, ветрогенераторы);

• внешние (наружные) и внутренние (потолочные, настенные, скрытые, встраиваемые) с углом обзора 360°, 180° и питанием 12/220 В;

• для камер, видеорегистраторов, видеоглазков, видеодомофонов;

• «ИК» – инфракрасные (тепловые, животных);

• беспроводные (сенсорные, микроволновые, лазерные, радиодатчики);

• автономных охранных пожарных сигнализаций (СМС в сотовом телефоне стандарта GSM, с сиренами звуковой, акустической и световой системы безопасности, шторы);

• автономные на батарейках и прочих элементах питания (электрические, пассивные);

• присутствия (уличные, открытия дверей, эхолоты);

• системы защиты от протечек (аквасторож, датчики утечки газа).

К установке рекомендуются прошедшие апробацию и признанные надежными (в наш турбулентный век мимикрий и различных эрзацев) датчики движения моделей LX-01, ДД-024, «Camelion», «Iek» (читается как Иэк), «Астра», «Colt», «Рапид», приемник электронных сигналов беспроводной сигнализации Merlin Pro, ИК детекторы присутствия, сирены, тревожные GSM кнопки (паники), датчики (протечки воды, разбития стекол, магнитоконтактные), пожарные извещатели.

Понимание того, что охранная сигнализация – это необходимость, а не очередная блажь богатых, доказано неоднократно практикой. Но и сегодня еще многие стараются сэкономить на ней, покупая самые простые и дешевые модели. Обычно они не отличаются высокой надежностью и часто приводят к ложным срабатываниям. Избежать этого можно только выбрав датчики от надежного производителя, которые рекомендовал выше.

1.8. Другие проводные датчики

К таким «второстепенным» элементам охранной системы относятся датчики открытия двери/окна. Датчики к системам «Sapsan» и «Mega SX» на примере датчика открытия двери/окна представлены на рис. 1.11.

Рис. 1.11. Дополнительный датчик, реагирующий на открывание окна

Датчик открытия двери геркон – это магнитно-контактный датчик, который срабатывает на размыкание.

Глава 2
Сравнительные характеристики элементов сигнализаций

В этой главе поговорим о разных элементах охранной сигнализации, которые совместимы в различных устройствах охранных сигнализаций (различных производителей).

2.1. Проводные GSM сигнализации и приемно-контрольные приборы

Проводные сигнализации – это охранные системы, которые строятся на базе кабельных соединений всех датчиков, оповещателей, приемно-контрольных приборов (ППКОП) или охранных централей. Назначение охранной сигнализации – это контроль доступа или событий в охраняемом помещении и оповещение о всех событиях либо при помощи GSM канала, либо при помощи других способов оповещения (световых или звуковых, вывода информации на пульт мониторинга или ПК и прочее).

Проводные системы безопасности позволяют при помощи датчиков, подключенных кабельными линиями, отслеживать движение, задымление, открытие, затопление, разбитие, вибрацию, изменение угла наклона или температуру. Широкий круг возможностей позволяет строить системы безопасности любой сложности, интегрировать несколько систем в единое целое, стыковать с существующим оборудованием, производить логические последовательности действия, отталкиваясь от фиксированных событий в системе.

Для примера рассмотрим приемно-контрольный охранно-пожарный прибор Астра-812МВ (плата базовая), который включает в себя:

- работу в составе системы Астра-РИ-М;
- контроль до 192 радиоканальных извещателей в составе системы Астра РИ-М;
- два проводных ШС (шлейфа);
- слоты для модулей: РПП Астра-РИ-М, Астра-МИП, Астра-PSTN;
- программирование с ПК или клавиатуры;
- голосовое сопровождение действий.

2.1.1. Сигнализации для производственных помещений (магазинов)

GSM проводная система – это доступная сигнализация для магазина, установка которой позволяет обеспечить ему круглосуточную охрану. Пакет услуг включает неограниченное

количество выездов вооруженного наряда охранников по сигналу «тревога». Контроль над технической исправностью сигнализации также осуществляется круглосуточно. Система предполагает прокладку проводов на объекте.

GSM радиоканальная система – это система беспроводная, монтируется быстро, работает бесперебойно, хотя и нуждается в периодической замене элементов электропитания. Достоинством данной беспроводной GSM сигнализации, в первую очередь, является оперативность монтажа. Для установки беспроводной GSM сигнализации достаточно одного дня.

Кроме того, данная беспроводная GSM сигнализация может быть установлена в любом помещении. Единственное требование – чтобы оно находилось в зоне действия сети оператора сотовой связи. Но не лишена эта беспроводная GSM сигнализация и недостатков. К таковым, в частности, следует отнести необходимость регулярной замены элементов питания, а также обязательное наличие сим-карты сотового оператора. Все это увеличивает расходы на эксплуатацию системы, но на самом деле, незначительно.

К примеру, ТЛФ-проводная система является эффективной сигнализацией для магазина, не нуждающаяся в автономных элементах электропитания и сим-карте сотового оператора связи. Устанавливается на объектах, имеющих стационарный городской телефон. Монтаж предполагает прокладку проводов. А GSM Ethernet проводная система использует для связи со станцией централизованного мониторинга сим-карту сотового оператора и интернет.

2.1.2. особенности проводной охранной сигнализации

Назначение любой охранной системы – предупреждение несанкционированного доступа в помещение любого типа. Сигнализация бывает проводной и беспроводной. Первая является наиболее распространенной и надежной, а стоимость на установку ее оборудования существенно ниже, чем для беспроводных систем, поэтому рассмотрим ее главные особенности.

Преимущества проводной сигнализации, не отмеченные ранее

По сравнению с другими типами охранной сигнализации, активно завоевывающих рынок охранных услуг в наши дни, проводная сигнализация существует уже десятки лет. За этот продолжительный период были выявлены, учтены и устранены все явные и неявные недостатки. Поэтому проводная охранная сигнализация, пожалуй, самая надежная охранная система из всех существующих на сегодняшний день. В этом и заключается главное ее преимущество.

Помимо этого, у проводной сигнализации есть также следующие основные особенности:

• обеспечение приборов на большом расстоянии питанием электроэнергией;

• полный контроль целостности связи без применения дополнительных технических средств;

• почти полное исключение электромагнитных помех;

• двухсторонний обмен данными;

• возможность проверки связи на обрыв линии;

• относительно недорогое оборудование;

• эксплуатация при неблагоприятных погодных условиях.

Недостатки проводной сигнализации, не отмеченные ранее

Несмотря на большое количество преимуществ, проводные охранные сигнализации обладают следующими недостатками:

• высокая стоимость монтажных работ, связанных с прокладкой линии связи;

• при большом количестве деталей коммуникаций нарушается интерьер помещения;

• подверженность линии связи намеренным или случайным механическим

повреждениям.

2.1.3. Разновидности проводных сигнализаций

Часто охранные организации при установке проводных сигнализаций на объект предлагают его владельцу интегрировать ее с всевозможными системами безопасности:

- анализаторами утечки газа и воды;
- противопожарными датчиками;
- системой контроля доступа;
- видеонаблюдением.

Применение проводной сигнализации

Разновидность охранной системы применяется без каких-либо ограничений практически на всех объектах, расположенных поблизости с коммуникативными центрами. Вдали от города проводная сигнализация подчас не выгодна из-за большого расхода на монтаж линии связи.

Проводной датчик наклона/удара «DST» представляет собой охранный извещатель, предназначенный для определения угла наклона охраняемого объекта и регистрации внешних воздействий (ударов, перемещений, вибраций) на объект. Акселерометр «DST» имеет выход для подключения к приемо-контрольному устройству и может применяться в составе любой охранной системы.

Прибор имеет настраиваемые пороги срабатывания по амплитуде ускорения, величине и времени наклона. При достижении порогового значения выход извещателя принимает разомкнутое состояние, при отсутствии воздействия выход находится в замкнутом состоянии. Для настройки необходим кабель Micro-USB.

Основные технические характеристики

Тип датчика…….. 3-осевой интегральный акселерометр
Порог срабатывания по наклону……. от 0 до 45°
Задержка срабатывания при наклоне… от 1 до 20 сек
Чувствительность по наклону…… 3°
Порог срабатывания по удару…… до 2 Дж
Интерфейс для связи с ПК…….. USB
Выход для подключения к охранному оборудованию……. 1 нормально замкнутый выход
Питание…….. DC 8—30 В; 5 В (USB)
Ток потребления…… 20 мА (при DC 12 В)
Габаритные размеры…… 70 х 30 х 22 мм
Диапазон рабочих температур…… от —30 до +50 °С

2.2. Справочные данные других датчиков – элементов охранных систем

2.2.1. CLIP-4N (производитель «Visornc»)

Это цифровой, сверхминиатюрный ПИК извещатель с областью обнаружения 6 х 3,6 м, линза «шторка»; регулировка дальности 6 м, 4 м и 2 м; алгоритм обработки True Motion Recognition и Digital FM Processing; питание 8…16 В/8 мА; размеры 70 х 28 х 25 мм.

2.2.2. Потолочный датчик движения DISC (производитель «Visonic»)

Это потолочный ПИК извещатель, область обнаружения (высота установки 4,5 м) – круг диаметром 9 м, 360°; алгоритм обработки True Motion Recognition; размеры 24 х 86 мм.

2.2.3. Устройство DUO 240 (производитель «Visonic»)

Потолочный комбинированный ПИК и СВЧ извещатель, область обнаружения (высота установки 4,5 м) – круг диаметром 9 м; алгоритм обработки True Motion Recognition; размеры 24 х 86 мм.

2.2.4. Устройство NEXT (производитель «Visonic»)

Цифровой датчик. Область обнаружения: 12 х 12 м, 90°, сферическая линза (9 + 5 шторок) с защитой нижней зоны, 2-эл. сенсор, 9…16 В, 8 мА, – 10…+50 °С; алгоритм TMR, микропроцессор; температура —10…50 °С; размеры 95 х 64 х 49 мм.

2.2.5. PATROL-101 (производитель «GSN»)

Извещатель охранный комбинированный ИК+СВЧ уличный, с обогревателем, рабочая температура —30…+60 °С/—55…+60 °С. Назначение изделия: уличный извещатель PATROL 101 предназначен для использования вне помещений, а также для эксплуатации в сложных климатических условиях при низких температурах, доходящих до —55 °С. Устройство создает узкую зону обзора, позволяющую свободное перемещение владельца объекта внутри защищаемого пространства.

PATROL 101 с функцией антимаскирования и датчиком смещения обнаруживает все попытки маскирования или нейтрализации извещателя путем смещения его со стены. Игнорирует животных массой до 30 кг.

Особенности устройства

Применение двойной технологии пироэлектрического детектора и СВЧ обеспечивает стабильное обнаружение, исключает ложные тревоги и, как следствие, дорогостоящие выезды на объект. Датчик оборудован встроенным обогревателем для использования в низкотемпературных климатических условиях, доходящих до —55 °С.

Датчик смещения обнаруживает внешние физические воздействия на извещатель. При ударе или попытке отрыва извещателя от стены устройство формирует тревожное сообщение и передаёт его на контрольную панель. Система антимаскирования обнаруживает любую попытку нейтрализации извещателя посредством экранирования (маскирования его с помощью материалов, блокирующих прохождение инфракрасной энергии на пироэлемент извещателя) и формирует тревогу. Выбор необходимого количества импульсов 1.7 предоставляет пользователю возможность оптимизировать чувствительность извещателя в соответствии с условиями окружающей среды для более стабильной работы прибора. Температурный компенсатор автоматически подстраивает работу извещателя к любым изменениям температуры окружающей среды. Экранирование пироэлемента обеспечивает высокую защиту от ложных срабатываний, которые могут быть вызваны источниками яркого света. Совершенная защита электронной схемы от RF и EM помех. В достоинства прибора необходимо добавить и механическую защиту пироэлектрического сенсора от RF помех.

Ударопрочный корпус извещателя выполнен из материала ASA-пластик, обеспечивающего стойкость к резким перепадам температур и, как следствие, продолжительный срок службы. PATROL-101 герметичен, пыленепроницаем и защищен от попадания водяных струй (IP65).

Устройство PATROL-101 ver. 2 является новой более усовершенствованной версии описанного выше устройства. Краткое описание: комбинированный ИК+СВЧ, 15 м, 90°; иПит 9…16 В; 1ПОТРтах 120 мА; уличный IP65; tpjAB —30…+60 °С; 55 х 49 х 153 мм; вес 270 г.

2.2.6. Устройство «Карат» (производитель «Сибирский Арсенал»)

Комплектация устройства: центральный блок (ЦБ) + блок индикации и управления (БИУ) – в одном корпусе; 24 зоны (расширение до 250 ШС); журнал событий (30 000); дальность распределения системы по проводному интерфейсу не менее 1 км; 4 ПЦН; эл. ключ; под аккумулятор 7 А/ч.

В состав устройства «Карат» входят центральный блок, выносной блок индикации и управления и адресные модемы для обеспечения связи между ЦБ и БИУ по адресной двухпроводной линии.

Центральный блок (ЦБ) + блок индикации и управления (БИУ) представлены на рис. 2.1.

Рис. 2.1. Внешний вид устройств «Карат» и «Карат-М»

Прибор «Карат» с БИУ предназначен для охраны различных объектов, оборудованных электроконтактными и токопотребляющими охранными и пожарными извещателями. Устройство обеспечивает оперативный мониторинг состояния средних и больших объектов, сохранение информации в виде журнала событий и отображение текущего состояния объектов.

2.2.7. Устройство «карат-м» (версия «карат»)

Краткое описание: центральный блок (ЦБ) в металлическом корпусе + блок индикации и управления (БИУ); 24 зоны (расширение до 250 ШС); журнал событий (30 000); дальность распределения системы по проводному интерфейсу не менее 1 км; 4 ПЦН; эл. ключ; под аккумулятор 12 А/ч (внешний вид см. рис. 2.1).

2.2.8. Устройство «С2000» (производитель «Болид»)

Краткое описание: пульт контроля и управления

1…127 приборов «Сигнал-20», «Сигнал-20П», «С2000-4», «С2000-КДЛ», «С2000-СП1», «С2000-К», «С2000-КС», «С2000-БИ», «С2000-ИТ», «С2000-АСПТ», «С2000-КПБ» по интерфейсу RS-485, архив событий, выход на ПЭВМ или принтер по RS.

Назначение изделия: прибор «С2000» предназначен для работы в интегрированной системе мониторинга и управления такими приборами и их модификациями, как «Сигнал-20», «Сигнал-20М», «Сигнал-20П», «С2000-4», «С2000-КДЛ», «С200 °СП1», «С2000-2», «С2000К», «С2000-КС», а также в системе АРМ «ОРИОН».

Особенности устройства:

• контроль до 127 приборов, подключенных к пульту по интерфейсу RS-485;

• отображение на ЖКИ, хранение в энергонезависимом буфере всех происходящих в системе событий и печать их принтере с последовательным интерфейсом RS-232;

• сигнализация тревог на встроенном звуковом сигнализаторе;

• управление взятием/снятием и контроль состояния шлейфов сигнализации с пульта;

• программирование конфигурационных параметров приборов, печать конфигурации на принтере, настройка адресов приборов и адресных устройств;

• ограничение доступа к функциям управления и программирования с помощью паролей.

На рис. 2.2 представлен внешний вид устройства.

Рис. 2.2. Внешний вид устройств «С2000» и «С2000-К»

2.2.9. Модификация устройства «С2000-К» (производитель «Болид»)

Краткое описание: выдача в интерфейс RS-485 команд на взятие, снятие охранных, пожарных зон, команд на предоставление доступа, отображение сообщений. Работает с АРМ «Орион». Внешний вид см. на рис. 2.2.

Назначение изделия: клавиатура «С2000-К» предназначена для работы в составе системы охранно-пожарной сигнализации для управления постановкой на охрану, снятия с охраны, а также в составе систем контроля и управления доступом. Клавиатура предназначена для работы только с сетевым контроллером.

Особенности устройства: предназначено для работы в интегрированной системе безопасности «Орион».

2.2.10. модификация «С2000-БС» (производитель «Болид»)

Описание: пульт и клавиатура со светодиодными индикаторами на 20 охранных или пожарных зон (рис. 2.3).

Рис. 2.3. Внешний вид устройства «С2000-КС»

Назначение изделия: пульт контроля и управления охранно-пожарный предназначен для работы в составе системы охранно-пожарной сигнализации для контроля состояния и сбора информации с приборов системы, индикации тревог, управления взятием на охрану, снятием с охраны, управления релейными выходами.

2.2.11. Модификация «С2000-М» (производитель «Болид»)

Описание: пульт контроля и управления с двухстрочным ЖКИ индикатором, количество разделов – 511, шлейфов (зон) – 2048.

Назначение изделия: пульт контроля и управления «С2000-М» предназначен для работы в составе систем охранной и пожарной сигнализации для контроля состояния и сбора информации с приборов системы, ведения протокола возникающих в системе событий, индикации тревог, управления постановкой на охрану, снятием с охраны, управления автоматикой.

Глава 3
Сравнительные характеристики приемно-контрольных узлов и контроллеров охранной сигнализации

В этой главе поговорим о разных центральных модулях охранной сигнализации, которые продаются, монтируются и обслуживаются сегодня. Эти модули, анализирующие электронные сигналы от нескольких (максимально не ограничено, но на практике – до нескольких сотен) различных датчиков, подключенных в системе, также принято называть контроллерами охранной сигнализации. Несмотря на то, что принцип их работы един, каждый такой модуль имеет и свои особенности, что необходимо учитывать специалисту (монтажнику, установщику) в индивидуальных практических условиях и конкретных задачах обеспечения безопасности.

3.1. Мираж-GE-iX-OI

Контроллер «Мираж-GE-iX-OI» предназначен для интеграции с приемно-контрольным оборудованием сторонних производителей (ВОРС «Стрелец», ИСО «Орион», радиосистема «Астра-РИ-М», а также различные системы, передающие данные по протоколу Contact ID).

Интеграция с периферийными устройствами (датчиками) в данном случае осуществляется на уровне протоколов, благодаря чему достигается максимально возможная информативность. Контроллер передает извещения от стороннего оборудования на ПЦН «Мираж» и позволяет подавать стороннему оборудованию команды с ПЦН «Мираж». Устройство оснащено двумя цифровыми входами, к которым можно подключить цифровые ШС для организации тамперной зоны или стационарной кнопки тревожной сигнализации. Наличие реле коммутации 12 В позволяет выполнять рестарт объектового прибора интегрируемой системы в случае его «зависания».

Передача извещений на ПЦН «Мираж» осуществляется по беспроводным сетям стандарта GSM 900/1800 (методы передачи данных TCP/IP GPRS, CSD, SMS), а также по проводной сети Ethernet без дополнительного оборудования. Алгоритмы работы оптимизированы для использования современных высокоскоростных технологий связи.

Рис. 3.1. Внешний вид контрольной панели «Мираж-ОБ-iX-01»

Устройство выполнено в компактном пластиковом корпусе с датчиком вскрытия. Для удобства установки предусмотрена возможность крепления на DIN-рейку. Модульная конструкция предусматривает подключение проводов к переходной клеммной панели, что значительно упрощает обслуживание и ремонт. На рис. 3.1 представлен внешний вид контрольной панели «Мираж-GE-iX-01».

3.1.1. Функциональные возможности

Функциональные возможности предполагают особенности системы передачи извещений:

- поддержка двух сетей связи стандарта GSM/GPRS 900/1800;
- поддержка сети стандарта Ethernet;
- непрерывный контроль работоспособности каналов связи;
- две GSM-антенны с автоматическим переключением: внутренняя планарная и внешняя, подключаемая к разъему SMA;
- собственный протокол MSRV, обеспечивающий двухстороннее динамическое шифрование, максимальную надежность и управляемость онлайн-каналов связи.

Приемно-контрольная панель имеет индивидуальные особенности:

• два цифровых входа контроля, предназначенных для приема извещений от приборов охранно-пожарной сигнализации;

• управление используемым при интеграции оборудованием;

• датчик вскрытия корпуса;

• реле коммутации 12 В.

Интеграция:

• интеграция с системой «Стрелец» осуществляется по интерфейсу RS-232;

• интеграция с радиосистемой «Астра РИ-М» производства компании ЗАО «НТЦ «ТЕКО» по интерфейсу LIN;

• интеграция с объектовой частью ИСО «Орион» производства НВП «Болид» при помощи преобразователя протоколов «С2000-ПП» по интерфейсу RS-485;

• интеграция с приемно-контрольным оборудованием сторонних производителей, использующих протокол передачи данных Contact ID, по каналу PSTN.

Сервисные возможности:

• индивидуальное программное обеспечение для каждого вида интеграции;

• дистанционная настройка объектового оборудования, постоянный контроль его работоспособности;

• дистанционная или локальная замена программного обеспечения контроллера;

• локальное конфигурирование через USB-интерфейс;

• удаленное конфигурирование по каналам TCP/IP GPRS, DATA (CSD) и Ethernet;

• встроенная система диагностики «Мираж-Suite»;

• сохранение информации в журнал событий;

• крепление на DIN-рейку или саморезы.

Питание:

• питание от адаптера 5 В / 1 А из комплекта поставки или внешнего БИРП напряжением 12 В;

• контроль напряжения внешнего источника питания;

• встроенная АКБ емкостью 1800 мА/ч.

3.1.2. Основные технические характеристики

Основные технические характеристики устройства «Мираж-GE-iX-Ol» таковы:

Максимальный ток
нагрузки выхода +12 В…….. 100 мА
Реле коммутации 12 В…….
Ток потребления в дежурном режиме… 350 мА
Ток потребления максимальный…….. 550 мА
Диапазон рабочих температур…… от 0 до +55 °С
Габаритные размеры…… 210 х 118 х 44 мм
Корпус……. ABS-пластик

Комплект поставки включает в себя:

• контроллер «Мираж-GE-iX-01» и руководство по эксплуатации на групповой комплект;

• внешний блок питания (5 В /1 А);

• паспорт (инструкция по эксплуатации);

• телефонный удлинитель, 2 м;

• аккумуляторная батарея (Li-Po, 1800 мА-ч);

• программное обеспечение на компакт-диске рассчитано на групповой комплект.

3.2. Мираж-GSM-iT-01

«Мираж-GSM-iT-01» – бюджетный контроллер, предназначенный для интеграции ИСМ «Мираж» с приемно-контрольным оборудованием сторонних производителей («Стрелец», ИСО «Орион», «Астра-РИ-М»). Интеграция осуществляется на уровне протоколов, благодаря чему достигается максимально возможная информативность.

Контроллер передает извещения от стороннего оборудования на пульт централизованного наблюдения «Мираж» и позволяет подавать стороннему оборудованию команды с пульта централизованного наблюдения (далее – ПЦН) «Мираж». Для выбора типа интеграции достаточно переключить микропереключатели на плате контроллера. По умолчанию прибор выпускается под интеграцию с системой охраны «Стрелец».

Передача извещений на ПЦН «Мираж» осуществляется по беспроводным сетям стандарта GSM 900/1800 (методы передачи данных TCP/IP GPRS, CSD, SMS). Контроллер имеет встроенную планарную GSM-антенну и возможность подключения внешней GSM-антенны. Реализован алгоритм автоматического переключения с внешней антенны на внутреннюю.

На рис. 3.2 представлен внешний вид контроллера «Мираж-GSM-iT-01».

Рис. 3.2. Внешний вид контроллера «Мираж-GSM-iT-01»

Надо заметить, что использование современной элементной базы и четырехслойной печатной платы позволило выполнить прибор в компактном корпусе.

3.2.1. Функциональные возможности контроллера «Мираж-GSM-iT-Ol»

Система передачи извещений включает в себя:

• поддержку двух сетей связи стандарта GSM/GPRS 900/1800;

• непрерывный контроль работоспособности каналов связи;

• две GSM-антенны с автоматическим переключением: внутренняя планарная и внешняя, подключаемая к разъему SMA;

• многоуровневая система защиты от несанкционированного удалённого доступа;

• передача на ПЦН «Мираж» извещений от приборов охранно-пожарной сигнализации в автоматическом режиме и прием команд управления от ПЦН «Мираж» в ручном режиме с квитированием обмена;

• надежная доставка информации с использованием оригинальных алгоритмов

оповещения, основанных на тестировании и резервировании каналов связи, адаптивном выборе методов передачи информации;

• интенсивное тестирование работоспособности оборудования и каналов связи во всех режимах работы контроллера для своевременного выявления неисправностей и возможного создания радиопомех (подавления);

• собственный протокол MSRV, обеспечивающий двухстороннее динамическое шифрование, максимальную надежность и управляемость онлайн-каналов связи.

Приемно-контрольная панель имеет следующие особенности:

• датчик вскрытия корпуса;

• встроенный порт mini-USB;

• интеграция с ВОРС «Стрелец» производства ЗАО «Аргус – Спектр;

• интеграция с радиосистемой «Астра РИ-М» производства компании ЗАО «НТЦ «ТЕКО»;

• интеграция с объектовой частью ИСО «Орион» производства НВП «Болид» при помощи преобразователя протоколов «С2000-ПП».

Сервисные возможности:

• дистанционная или локальная замена программного обеспечения контроллера;

• локальное конфигурирование через USB-интерфейс;

• удаленное конфигурирование через TCP/IP GPRS и DATA (CSD);

• встроенная система диагностики «Мираж-Suite»;

• сохранение информации в журнал событий.

Особенности подключения питания:

• подключение от внешнего бесперебойного источника питания;

• контроль напряжения внешнего источника питания.

3.2.2. Основные технические характеристики

Основные технические характеристики контроллера «Мираж-GSM-iT-Ol» таковы:

Количество сетей связи
стандарта GSM/GPRS…… 2
Период тестирования каналов связи…. от 10 сек
Время доставки извещений……. 1–2 сек (TCP/IP)
Основное напряжение питания…… 12 В
Диапазон рабочих температур…… от —40 до +55 °С
Габаритные размеры…… 90 х 70 х 23 мм
Материал корпуса……. ABS-пластик

3.3. Мираж-GE-RX4-02

Контроллер «Мираж-GE-RX4-02» предназначен для пультовой охраны малых и средних объектов недвижимости (офисы, небольшие магазины, павильоны, банкоматы, складские помещения, пультовая охрана частной недвижимости).

Благодаря компактности и поддержке радиоизвещателей контроллер является идеальным решением для использования в квартирах (может устанавливаться в помещениях с законченным ремонтом без ущерба для их эстетического вида).

Контроллер поддерживает одновременное подключение до четырех ШС с пороговыми охранными и технологическими извещателями и до 28 радиоизвещателей и ретрансляторов «Ладога-РК». ШС и радиоизвещатели могут распределяться по четырем логическим разделам с независимой постановкой на охрану. Возможность подключения устройств для расширения количества ШС и разделов не предусмотрена. Контроллер оснащен тремя

выходами управления типа «открытый коллектор».

На рис. 3.3 представлен внешний вид контроллера «Мираж-GE-RX4-02».

Передача извещений на ПЦН «Мираж» осуществляется по беспроводным сетям стандарта GSM 900/1800 (методы передачи данных TCP/IP GPRS, CSD, SMS) и сети Ethernet без дополнительных устройств. Алгоритмы работы оптимизированы для использования современных высокоскоростных технологий связи.

Устройство выполнено в компактном пластиковом корпусе с датчиком вскрытия. Для удобства установки предусмотрена возможность крепления на DIN-рейку. Модульная конструкция предусматривает подключение проводов к переходной клеммной панели, что значительно упрощает обслуживание и ремонт.

Функциональные возможности

Функциональные возможности рассмотрим, начиная с системы передачи извещений:

• поддержка двух сетей GSM/GPRS 900/1800;

• поддержка сети стандарта Ethernet;

• непрерывный контроль работоспособности каналов связи;

• многоуровневая система защиты от несанкционированного удалённого доступа;

• собственный протокол MSRV обеспечивает двухстороннее динамическое шифрование, максимальную надежность и управляемость онлайн-каналов связи;

• две GSM-антенны с автоматическим переключением: внутренняя планарная и внешная, подключаемая к разъему SMA.

Рис. 3.3. Внешний вид контроллера «Мираж-GE-RX4-02»

Приемно-контрольная панель включает в себя:

• четыре конфигурируемых шлейфа сигнализации (ШС) для приема извещений от охранных извещателей;

• четыре раздела для отдельной постановки собственных ШС;

• возможность одновременной постановки/снятия всех четырех собственных ШС;

• возможность поразделной постановки шлейфов, в четыре раздела можно объединять как собственные ШС, так и радиодатчики «Ладога– РК»;

• управление исполнительными устройствами и средствами автоматики с помощью трех выходов управления типа «открытый коллектор»;

• питание выходов управления типа «открытый коллектор» осуществляется через внешний либо встроенный источник;

• управление режимом работы с помощью электронных ключей Touch Memory, бесконтактных считывателей, скрытых выключателей, кодовых панелей, электронных ключей с шифрованием (DS1961S);

• настраиваемая для любого выхода звуковая/световая индикация поразделной постановки ШС;

• звуковая и световая сигнализации в режимах «Тревога» / «Неисправность»;

• световая индикация номера ШС, в котором произошло срабатывание извещателя;

• восемь тактик управления цепями звуковой и световой сигнализации;

• контроль вскрытия корпуса.

Интеграция с беспроводной радиосистемой «Ладога-РК» за счет встроенного радиомодуля (поддержка до 28 датчиков).

Сервисные возможности:

• дистанционная или локальная замена программного обеспечения контроллера;

• локальное конфигурирование через USB-интерфейс и удаленное конфигурирование через TCP/IP, Ethernet и DATA (CSD);

• встроенная система диагностики «Мираж-Suite»;

• сохранение информации в журнал событий;

• крепление на DIN-рейку или саморезы;

• съемная клеммная панель для удобства монтажа и обслуживания.

Питание:

• питание от адаптера 5 В/1 А из комплекта поставки или внешнего БИРП напряжением 12В;

• встроенная Li-Po АКБ емкостью 1800 мА/ч.

Комплектность устройства:

• контроллер «Мираж-GE-RX4-02»;

• паспорт (руководство пользователя);

• электронный ключ;

• резистор;

• внешний блок питания (5 В /1 А);

• аккумуляторная батарея Li-Po 1800 мА/ч;

• радиоантенна 433 МГц;

• программное обеспечение.

3.4. Мираж-GSM-A8-03

Контроллер «Мираж-GSM-A8-03» позволяет решать самые масштабные задачи частного охранного, пожарного и технологического мониторинга недвижимости (квартиры, коттеджи, неотапливаемые дачи и гаражи, комплексы построек) с применением как проводных, так и радиоканальных извещателей. Извещения передаются на сотовые телефоны пользователей (до восьми телефонных номеров) в виде SMS-сообщений и голосовых звонков. Реализована возможность передачи извещений на ПЦН «Мираж» по каналу SMS.

Прибор поддерживает одновременное подключение до восьми собственных ШС с пороговыми охранными, пожарными и технологическими извещателями (в том числе с питанием по шлейфу). С помощью трансивера «Мираж-TR433» к контроллеру подключается до 32 радиоизвещателей и ретрансляторов «Ладога-РК». ШС и радиоизвещатели можно распределять по четырем логическим разделам с независимой постановкой на охрану.

Кроме того, контроллер позволяет реализовать функции «умного дома» (контроль

внутренней среды помещения с помощью технологических извещателей и термодатчиков, регулировка температуры, автоматическое и дистанционное управление различными устройствами). Он оснащен четырьмя выходами типа «открытый коллектор», которые предназначены для управления устройствами локального свето-звукового оповещения и (с помощью блока силовых реле «Мираж-БРЗ») сильноточными исполнительными устройствами. Имеется встроенный датчик температуры, возможно подключение четырех дополнительных датчиков температуры и микрофона. Подключение микрофона позволяет осуществлять дистанционное прослушивание помещения через сотовый телефон. Возможно применение различных локальных и дистанционных методов конфигурирования и управления режимом охраны. Реализован автоматический контроль финансового баланса установленных в контроллер SIM-карт.

Устройство является функционально и конструктивно законченным изделием, выполненным в пластиковом корпусе с датчиком вскрытия. Он включает в себя систему передачи извещений по двум сетям стандарта GSM/GPRS-900/1800, приемно-контрольную панель и источник бесперебойного питания. Питание осуществляется от сети 220 В, в качестве резервного источника предусмотрено использовать аккумуляторную батарею емкостью 7 А/ч.

3.4.1. Функциональные возможности

Система передачи извещений:

• поддержка двух сетей сотовой связи GSM/GPRS 900/1800;

• оповещение о системных и тревожных событиях с помощью SMS-сообщений и голосовых звонков;

• передача SMS-сообщений в формате Call ID на ПЦН «Мираж»;

• автоматический контроль возможного подавления каналов связи техническими средствами, многоуровневая система защиты от несанкционированного удалённого доступа.

Приемно-контрольная панель:

• восемь входов для подключения шлейфов охранной, пожарной и технологической сигнализации, каждому из которых могут быть назначены различные тактики и атрибуты использования;

• произвольное распределение ШС и радиоизвещателей по четырем логическим разделам;

• четыре выхода управления типа «открытый коллектор»;

• контроль вскрытия корпуса;

• локальное управление режимом охраны с помощью кодовой панели «Мираж-КД-03», считывателя электронных ключей Touch Memory, скрытого выключателя, кнопки;

• контроль температуры в помещении с помощью встроенного и дополнительных термодатчиков;

• акустический контроль помещения с помощью внешнего микрофона.

3.4.2. Сервисные возможности

Сервисные возможности:

• конфигурирование контроллера и обновление встроенного программного обеспечения с помощью программы «Конфигуратор Приват» с подключением локально через USB-интерфейс или удаленно по каналу TCP/IP GPRS;

• дистанционное управление контроллером с помощью голосового меню, SMS-команд, программы «Конфигуратор Приват», мобильного приложения Private Mobile;

• автоматический контроль баланса финансовых средств на SIM-картах контроллера, оповещение о снижении баланса ниже установленного порога.

Особенности электропитания:

• широкий диапазон напряжения основного электропитания;

• аккумуляторная батарея емкостью 7 А/ч, автоматический заряд, защита от переполюсовки и глубокого разряда;

• автоматическое переключение электропитания с основного источника на резервный (АКБ) и обратно без выдачи ложных сигналов на выходы управления и по каналам оповещения.

Основные технические характеристики

Количество сетей связи стандарта
Количество ключей Touch Memory
и/или кодов…….. 8
Количество выходов управления……. 4
Напряжение в ШС…… 4 В; 24 В
Электропитание основное…… 85—264 В
Электропитание резервное от АКБ……. 12 В, 7 А ч
Максимальный ток нагрузки……. 700 мА
Диапазон рабочих температур…… от —40 до +55 °С
Габаритные размеры…… 260 х 180 х 85 мм
Материал корпуса……. ABS-пластик

Комплект поставки:

• контроллер «Мираж^$M-A8-03»;
• электронный ключ DS1990A (2 шт.);
• GSM-антенна «Mirage-AMG»;
• кабель USB 2.0 A – B (1,8 м);
• резистор CF-0.25 (5,6 кОм) (8 шт.);
• программное обеспечение и документация на компакт-диске;
• паспорт изделия и краткое руководство по эксплуатации;
• инструкция «Быстрый старт».

3.5. Проводная охранная система «Контакт GSM-5-RT1»

Устройство «Контакт GSM-5-RT1» предназначено для приема сигналов от охранных панелей любых иностранных и отечественных производителей и последующей передачи на пульт централизованного наблюдения охранного предприятия.

Внимание, важно!

Основной уникальный принцип, реализованный в «Контакт GSM-5-RT1», – это преобразование аналоговых сигналов, поступающих от объектовых охранных панелей, в цифровое представление непосредственно на объекте, а затем передача по различным каналам связи на пульт уже цифрового сигнала.

Многие устройства пытаются передавать через сеть GSM аналоговый сигнал, что является непростительной ошибкой для любого оборудования, так как аналоговый протокол Ademco ContactID не приспособлен для передачи через сотовую сеть. Выход очевиден: преобразовать аналоговый сигнал в цифровой непосредственно на объекте и передать на пульт через сеть GSM или LAN непосредственно «цифру», именно данную задачу и решает «Контакт GSM-5-RT1».

Технические характеристики РИТМ «Контакт GSM-5-RT1»

Передача информации через GPRS…… есть
(2 SIM карты)

Передача информации
через цифровой канал GSM…… есть
(2 SIM карты)
Передача информации
через голосовой канал GSM…… есть
(2 SIM карты)
Передача информации через локальную сеть LAN и Internet
Передача информации через городскую телефонную сеть
Основной протокол
передачи информации…… Ademco ContactID
Удаленное программирование
10-14 В
Питание……..
Контроль наличия 220 В

3.6. Кодовая панель «Мираж-КД-03»

Кроме непосредственно контроллеров-модулей в системах охраны заслуживают внимание кодовые панели, предназначенные для ввода (с клавиатуры) кодов, по которым система идентифицирует владельца охраняемого помещения (доверенное лицо), распознает их и санкционирует команду на снятие/постановку системы в режим «охрана». Далее рассмотрим одну из таких панелей.

Кодовая панель «Мираж-КД-03» подключается к объектовому оборудованию «Мираж» для ввода кодов постановки объекта на охрану и снятия с охраны. Выполнена в пластиковом корпусе в двух цветовых вариантах – сером и черном. Отличается современным строгим дизайном, компактностью и удобной сенсорной клавиатурой с подсветкой и звуковым подтверждением нажатия. На панели расположены индикаторы состояния шлейфов сигнализации, питания и режима охраны.

Основные технические характеристики
Питание…….. 12 В
Интерфейс подключения Touch Memory
Максимальный ток потребления……. 50 мА
Диапазон рабочих температур…… от 0 до +55 °С
Габаритные размеры…… 112 х 67 х 16 мм
Материал корпуса……. ABS-пластик

Глава 4
Выявленные способы нейтрализации современных электронных охранных систем

В этой главе поговорим о том, каким способом можно защитить охранную систему от несанкционированного вмешательства. Инженерные решения могут быть выработаны именно исходя из знания проблемы, ведь это уже первый шаг к ее решению. По сути, в этой главе автор предлагает «Инструкции по борьбе со злоумышленниками».

4.1. Проблемы современных охранных сигнализаций: краткий обзор

С позиции антисоциальных элементов проникновение в охраняемые помещения тем более выгодно, чем больший финансовый вес имеют охраняемые ценности. С учетом необходимости блокирования установленных систем охраны проще всего проникать в

частное жилье граждан, ибо на промышленных объектах установлены более дорогие и многофункциональные системы охраны. Преодолеть их защиту сложнее из-за необходимости затрат на оборудование, но возможно.

Более того, сегодня все охранные системы помещений работают по одному принципу и состоят, как правило, из центрального модуля охраны с дисплеем и клавиатурой и подключаемых к нему датчиков различного назначения. Почти везде (безотносительно частного или промышленного сектора) устанавливают в качестве элементов системы – датчики движения на основе пироэлектрических детекторов (PIR).

Первые датчики движения стали широко доступны чуть более 10 лет назад. С тех пор они, разумеется, эволюционировали, но принцип их действия остался тем же – реакция на изменение температурного фона в контролируемой зоне. Они весьма просты, удобны, но обладают рядом недостатков, которые научились использовать в своих целях злоумышленники. В ряде случае не помогает даже аппаратная регулировка чувствительности пироэлектрического детектора.

Если рассматривать простой бытовой пример, то перемещение человека в помещении (в зоне контроля датчиков на основе пироэлектрического детектора) где включен газ (газовая горелка, кухонная плита) не вызывает у такого датчика никакой реакции. В этой связи участились случаи, когда страховые компании стали испытывать повышенную нагрузку в части страховых выплат, и как реакцию, стали практиковать новые «защищающие» пункты в договорах о страховании имущества, предполагающие дополнительные и не всегда оправданные требования к установке и обслуживанию систем безопасности. Это актуально особенно тогда, когда имущество учитывается в крупном размере. Все это породило цепную реакцию исследований и желания – с одной стороны найти дополнительные варианты защиты имущества посредством усовершенствования систем современной электроники, а с другой стороны, выяснить на что же способен и чего лишен сам пироэлектрический детектор.

Но проблема страховых компаний в том, что они пользуются услугами консультантов, выводы которых, в основном сделаны с опорой на теоретические размышления, а не на практику. Поэтому не всегда могут постфактум объяснить предметно – как произошел тот или иной случай. Потому многим компаниям, занятым в сфере исследований проблематики охранных систем, консультирования, аналитики, расследования страховых случаев нужны не просто теоретические выкладки (можно/нельзя блокировать), но, главное, практические выводы и рекомендации, основанные на обоснованных теорией экспериментах.

Для многих небольших компаний, занятых в означенной сфере, обращение в профильные институты и хлопотно и накладно. А кроме того, при такой практике обращений неизбежны потери времени. Бюрократический механизм работы и оформления выводов исследований неоправданно неповоротлив.

Кроме того, почти всегда при таких взаимоотношениях отсутствует возможность оперативно уточнить возникшие по заключению вопросы. В этой связи, конечно, удобнее работать с небольшими профессиональными консультационными организациями.

4.1.1. Европа и мы

Во многих странах Европы и Америки (также и Объединенного Королевства), где я побывал и изучил особенности ситуации, инженерами по связи и безопасности могут называться люди, образование которых находится на уровне электрика ПТУ во времена СССР. Здесь я не хотел бы никого обидеть; это оценочное суждение, позволительное в данном контексте автору, в соответствии с конкретным опытом и анализом увиденного за рубежом в период с 2010 года и по настоящее время. Англичане даже на уровне простого электрика в России, себя называют не иначе, как «инженер-электрик». И высоко квалифицированный специалист с опытом работы ценится не менее нашего кандидата наук.

С 2003 года в России, видимо для соответствия, унификации требований и

конкурентной способности в сравнении с Европой, принята Болонская система образования, теперь и у нас уровень бакалавра – лишь начальная ступень высшего образования. Впрочем, особенности систем образования не входят в задачи предметного рассмотрения данной книги. В Европе более всего имеют значение не регалии, («формальная остепененность»), а практически ориентированные знания, и настоящий консультант в области электронной техники даже здесь большая редкость. В период моих частых командировок я замечал, что у штатных специалистов работа ограничивается «блоками»: сменой платы на телевизоре, компьютере или вкручивания осветительной лампочки… по инструкции – по часовой стрелке.

С другой стороны самую высокую признательность здесь имеет не тот, кто «признан в научном сообществе» по формальным признакам соседства по работе и (или) количестве печатных публикаций, а, главным образом, по своим практически-ориентированным знаниям, опыту, который можно трансформировать в новые открытия, адаптировать к реальной, а не вымышленной ситуации. Выводы, которые понятны «здесь и сейчас», соответствуют функционалу и проблематике современного (а не прошлогоднего) оборудования, знания, которые можно практически интерпретировать.

Самое высокое звание в Европе, к примеру, не доктор искусствоведения в области литературы, а эксперт. И настоящих экспертов мало, а инженеров по связи – много. Более того, именно из Европы пошла «мода» на заслушивание Нобелевских лауреатов, с предоставлением им слова. Если человек не знает – о чем он говорит (даже при наличии нескольких «научных степеней»), экспертам это сразу станет ясно. На этот счет хорошо подходит и высказывание: «О чем бы человек ни говорил, он всегда говорит о себе».

Итак, с точки зрения эксперта разберем несколько случаев блокировки элементов охранной системы – датчиков движения, подключаемых к центральному блоку управления по проводам – пироэлектрических детекторов (PIR).

4.2. Особенности защиты шлейфа по проводной схеме

Начнем с того, что представим себе особенности оборудования на примере центральных блоков управления и обработки сигналов и периферийных датчиков (PIR), разумеется и других датчиков, которые система позволяет подключать для комплексной охраны (датчики разбития стекла, ИК-датчики, акустические датчики и др.). Модули охраны (центральный блок) выпускались и выпускаются разных моделей.

Рис. 4.1. Внешний вид центрального модуля фирмы Honeywell производства Канада

На рис. 4.1 представлен внешний вид центрального модуля фирмы HONEYWELL производства Канада.

Подключение к модулю производится по стандартной схеме – в соответствии с рекомендациями производителя. Исходя из задач охранной системы иногда к шлейфу охраны подключают только один, иногда несколько пироэлектрических детекторов. В устройстве центрального блока (рис. 4.1) с ЖКИ задействована LCD клавиатура КР-1002.

На рис. 4.2 представлен внешний вид центрального модуля DHS производства Канада. Это аналогичный (относительно DHS) по функционалу блок.

Кроме систем охраны, взаимодействующих с периферийными датчиками посредством проводных соединений (шлейфов), существуют беспроводные системы охраны, где пироэлектрические (PIR) датчики передают сигнал на частоте 2,4 ГГц, к примеру, DSC Wireless Pet Immune PIR Motion Sensor, представленный на рис. 4.3.

Устройства для беспроводной охранной сигнализации встречаются разные. Перечислять или приводить в пример все не представляется возможным, их расширенные возможности говорят за себя сами – один модуль может контролировать 99 и более зон ответственности (читай – помещений), передача сигнала беспроводным методом может быть не только на частотах 2,4 ГГц (это вообще – для бытовых назначений), но и на частоте 33 МГц (модуль WS9901 производства Великобритании).

Блокировать такие системы еще проще посредством включения в соседнем помещении электронного «генератора шума», работающего в том же диапазоне частот. Один из примеров такой «заглушки», всесторонне испытанной в лаборатории автора, представлен на рис. 1.2 – в первой главе книги. С таким устройством можно сделать временно бесполезными не только устройства, взаимодействующие на частоте 2,4 ГГц, но 900/1800 МГц (сотовая связь стандарта GSM), приглушить в конкретном месте и без того слабые сигналы спутников GPS.

Рис. 4.2. Внешний вид центрального модуля DHS производства Канада

Избежать этого можно комплексным подходом, установив несколько разных охранных датчиков, в том числе таких, которые контролируют ИК луч-барьер (нарушение луча приводит к срабатыванию датчика). Так злоумышленнику будет труднее заблокировать всю систему охраны, когда в ее составе будет несколько датчиков с разными функциональными особенностями.

Рис. 4.3. DSC Wireless Pet Immune PIR Motion Sensor модели WS4904 производства Канада.

Внимание, важно!

Именно поэтому серьезные организации устанавливают (и рекомендуют) только проводные системы охраны на основе PIR. Для того, чтобы быть в курсе событий в области охранных систем заинтересованному специалисту необходимо все время держать руку на пульсе инноваций в области современных электронных систем, в сегменте охраны и на основе PIR. Для этого мало изучения журналов соответствующей тематики (хотя это и важно, и полезно), необходимо участвовать в профильных конференциях, в том числе международных, или хотя бы изучать результаты исследований по данной теме [3].

Так или иначе опыт зарубежных и российских партнеров в этой области транслируется в открытом доступе. На мой взгляд, получить новейшие практические знания и передовой опыт, можно только общаясь на постоянной основе с коллегами на конференциях по проблематике электронных устройств охраны. Те, кто не жалеет на это современное знание материальных активов своих компаний, более защищены и менее подвержены неприятностям вследствие изучения проблематики постфактум – после случаев блокировки системы злоумышленниками.

Если несанкционированное проникновение в помещение происходит через крышу, как правило, выясняется, что монтаж систем охраны выполнялся не просто с нарушением регламента и требований по установке элементов системы, но и вопреки какой-либо логики: соединительные (шлейф) провода между основным блоком системы и периферийными датчиками проведены непосредственно по балкам, на недостаточной высоте, досягаемой с поверхности пола, и (или) кабель-каналы имеют свободный доступ для посторонних лиц.

В случае несанкционированного проникновения и ограбления магазинов, находящихся под охраной системы с пироэлектрическими датчиками движения, было замечено, что повреждена изоляция проводов от датчиков к основному блоку. Таким путем с помощью специально изготовленного «под заказ» электронного устройства «обманки-имитатора» был «шунтирован» сам датчик, чтобы сигнал при срабатывании не поступал на пульт охраны магазина и не передавался дальше пульта [2].

В таких случаях, учитывая разные модели производителей охранных систем с соответствующим функционалом, принимая во внимание особенности монтажа и подключения проводов между периферийными датчиками и центральным пультом охраны,

злоумышленниками проводится предварительная подготовительная работа с целью определения модели системы.

Также не исключена возможность преступной связи злоумышленников с монтажниками, то есть для «успешного» несанкционированного проникновения, безусловно, необходимы знания не только в области основ электротехники и навыки монтажных работ для изготовления электронного имитатора (далее ЭИ), но и о подробностях монтажа охранной системы. Возможно, таким лицом являлся или бывший работник, или человек хорошо информированный монтажниками системы.

Внимание, важно!

Дело в том, что на практике монтажники-установщики охранных систем могут по-разному подключать шлейф охраны, к примеру, красный проводник не всегда «+» питания, а зеленый – не всегда «открытый коллектор» с пироэлектрического детектора. Провода можно «зашифровать», подключив систему иначе, это дополнительный элемент защиты всей системы, а значит и ценностей, находящихся под ее охраной, который, безусловно, оправдывает себя.

В каждом конкретном случае надо разбираться предметно – как обстоят дела с безопасностью информации и ее несанкционированным распространением.

4.3. Универсальный способ блокировки

Некоего универсального способа подключения обманки-имитатора не существует, поэтому и важно знать – как именно подключены провода (цвета и прочие особенности монтажа). Утверждение монтажников о том, что при включенной системе этого сделать невозможно, отчасти верно. Но только отчасти.

Электронный имитатор-обманка, изготовленный без учета знаний о конкретике установленной системы бесполезен, поскольку это вызовет спад напряжения и сопротивления в шлейфе охраны, выработку сигнала «тревога». Даже подключение тестера (мультиметра в режиме измерения постоянного напряжения) к проводам шлейфа (если это только не провода «+» и «—» питания) вызовет импульс сигнала «тревога» в связи с высокой чувствительностью входного каскада центрального блока системы. Поэтому «грамотные обманщики» применяют электронный имитатор с очень высоким входным сопротивлением, чтобы ЭИ не шунтировал сигнальную цепь, при работающем устройстве (на элементы системы подано питание и включен режим «охрана») – на практике подключают одновременно несколько контактов (это не вдаваясь в детали устройства), а для того, чтобы «сработать без осечек» нужны определенные навыки у злоумышленника.

Внимание, важно!

Универсального устройства (обманки), которое бы блокировало широкий спектр охранных систем, созданных по принципу, рассматриваемому нами, не существует. Да если бы оно и было, уже все пересмотрели бы свои взгляды на организацию охраны с помощью таких систем. Если кто-то и блокировал обманкой по проводам, то видео в открытый доступ по понятным причинам выкладывать не станет.

Итак, можно ли практически это сделать, если предположить доступ к проводам, идущим от PIR к центральному модулю-пульту? Эту работу может провести специалист-установщик оборудования, тот, кто владеет компетенциями установки или недавно работал в этой области с такими же электронными модулями. Просто «вор с улицы» не способен разобраться в проводке, выделить из шлейфа проводов – значимые.

На сегодняшний день особый интерес вызывают PIR детекторы (пироэлектрические сенсоры, пироэлектрические датчики). Потому что их научились «обходить». Рассмотренные выше модели центральных модулей защищены (в том числе от вскрытия корпуса), и его злоумышленники, как правило, не трогают. Блокировка PIR-детекторов является наиболее

частой причиной несанкционированного проникновения в охраняемые помещения, поэтому PIR является самым уязвимым звеном всей системы.

И вот почему.

4.4. Воздействия на PIR

Дистанционное блокирование PIR-детекторов наиболее вероятно, когда они находятся в пределах видимости, имеется возможности их визуально контролировать, к примеру, адаптированный в России «Орлан-201» и его прообраз «Фотон-9» (рис. 4.4), а также датчик SEN24, имеющий в своем составе ту же электронную плату и условия коммутации внешних подключений (линий).

При выработке сигнала «тревога» большинство применяемых сегодня в охранных системах периферийных устройств с PIR индицируют свое состояние световыми вспышками вынесенного на переднюю панель светодиода, а некоторые устройства, к примеру, показанное на рис. 4.5, и др. еще и звуковым сигналом.

И эта наглядная индикация весьма помогает злоумышленнику контролировать состояние приборов (реакцию на воздействие в охраняемой зоне) дистанционно. Производитель (разработчик) добавил этот функционал не зря, для тестовых возможностей. Разумеется, вскрыв корпус датчика, и световую, и звуковую индикацию можно отключить с помощью перемычек-джамперов (работа монтажника системы), но не каждый установщик это сделает отрегулировав, протестировав систему после установки уровней чувствительности в конкретных условиях (помещении).

Таким образом, пресловутый «человеческий фактор» может повлиять на безопасность всей системы в долгосрочной перспективе. Отсюда вывод: для того, чтобы система обладала большей безопасностью «тестовую» индикацию после завершения монтажа и настройки требуется отключить. Даже если на окнах установлены герконовые (типа СМК) или акустические датчики (на разбитие стекла, открывание окна) для начального шага проникновения – блокировки PIR – не потребуется его вскрывать.

Рис. 4.4. Внешний вид и вид со снятой крышкой датчика «Орлан-201», работающего с системой охраны DHS (рис. 4.2) и др.

Итак, когда PIR находится в зоне видимости, на него можно воздействовать извне, то есть, в частности, через окно. Это важно для понимания последующих в разделе выводов. На международной конференции в Лас-Вегасе по проблематике электронных охранных систем BLACK HAT USA эксперт Bishop Fox (компания Drew Porter) тоже отметил [1] уязвимость PIR датчиков, их блокировку под воздействием инфракрасных лучей соответствующей длины. Я отработал эту версию практически. В этой связи возникают два практических вопроса. Можно ли ослепить PIR, чтобы не поступил сигнал от датчика на модуль? Можно

ли это сделать, если имеется доступ к проводам, идущим от PIR к модулю?

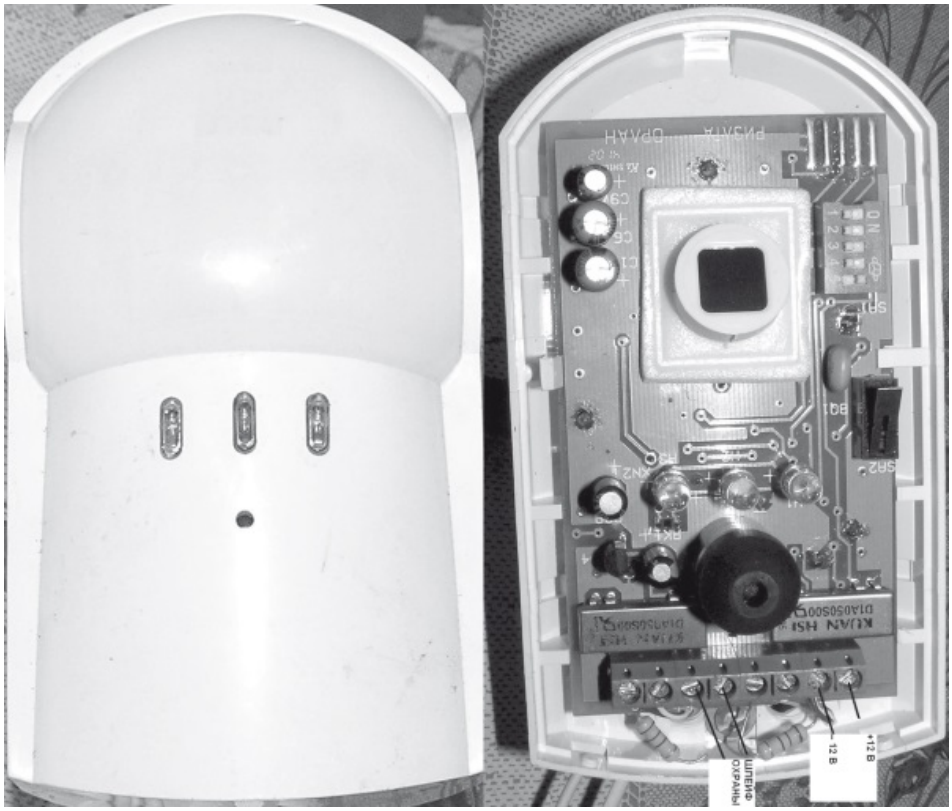

Рис. 4.5. Внешний вид устройства и вид со снятой крышкой датчика в системе охранной сигнализации Honeywell

ИК-лучи, источником которых может быть один или несколько, установленных на одной плате ИК светодиодов отражаются от стен помещения. В бытовых условиях это нетрудно заметить без дополнительной экспертизы: бытовая и иная техника, управляемая (в том числе) посредством ПДУ (где реализуется способ управления на ИК лучах) принимает команды, даже если пульт не направлен непосредственно на устройство бытовой техники.

Однако этого недостаточно для «ослепления» датчика, поскольку последний все равно будет контролировать зону ответственности. Причем важно понимать, что ИК-лучи не проходят через непрозрачные стены, а отражаются. Таким образом, источник сигнала должен быть направлен непосредственно на датчик, причем в самую его рабочую поверхность – на линзу Френеля. Если для этой цели применять «лазерные указки» и другую аппаратуру (даже мощную), но с сильно концентрированным фокусированным лучом, то тот, кто направляет должен иметь навыки. Стоит лишь незначительно отклонить луч лазера от рабочей поверхности датчика и «ослепление» становится не эффективно, то есть остается возможность выработки хотя бы одиночного импульса сигнала «тревога».

Если это лазер ИК спектра излучения (длины волны), он должен быть направлен непосредственно на датчик и удерживать луч на нем все то время, пока в помещении проводятся «несанкционированные работы». Тогда луч через линзу Френеля попадает на рабочую поверхность чувствительного пироэлектрического детектора, который преобразует изменение «теплового» фона в электрический ток. Причем на основе экспериментов, проведенных с разными датчиками в 2014 году, можно с уверенностью сказать, что в первый момент «ослепления» (воздействия) датчик все равно сработает, то есть однократная выработка импульса будет, а уже затем элемент PIR останется «слеп».

Значительно эффективнее «ослеплять» датчик с помощью не сконцентрированного пучка (луча, как лазер), а рассеянного света посредством устройства инфракрасной (ИК) подсветки.

Может ли быть использован мощный ИК светодиод для «ослепления» датчика из другого помещения, или он должен быть направлен напрямую на датчик?

Для применения устройства (в эксперименте, так как речь идет не о рекомендациях для «взломщиков») в нем принудительно отключают блокировку ночного режима – включение ИК диодов только при затемнении. Основной функционал устройства на примере SAL-10 (ее мощность 10 Вт, а есть и более мощные) – автомобильная подсветка для ночной видеосъемки видеорегистратором. При подключении к аккумулятору с напряжением 12 В она становится вполне автономной (переносной). Но из другой комнаты и оно не может «ослеплять». Сигнал отражается от стен, хотя с таким устройством, в отличие от пучка лазера, не обязательна точность направления на рабочую поверхность IR, достаточно примерного направления.

По той же причине нельзя устанавливать видеокамеры наблюдения (с функцией автоматической ночной подсветки) в том же помещении, если они направлены в сторону PIR, ибо с уменьшением освещенности в помещении автоматически включается ИК-подсветка, и это обстоятельство может провоцировать «ослепление» датчика, установленного в том же помещении, особенно, если оно по площади относительно небольшое. Все эти факторы вызовут сначала срабатывание датчика (ложное), а затем его «слепоту», пока есть воздействие ИК лучами.

4.5. Самый простой способ нейтрализации

Итак, PIR можно заблокировать даже самым простым способом – напылением на рабочую поверхность или с применением ИК лучей не направленного, а рассеянного источника. По той же аналогии, обычное накрывание датчика платком, тряпкой, на манер накрытия клетки с попугаем, полностью решает вопрос его нейтрализации.

Существуют возможности «ослепления» PIR воздействием радиоволнами. Эксперименты 2014 года, проведенные с различными радиостанциями и на различных частотах показали, что это не ослепление, а воздействие, но тем не менее, оно верно.

Можно добиться срабатывания датчика посредством воздействия включенными в режим «передача» радиостанциями, работающими в широком диапазоне радиоволн даже небольшой мощностью радиоизлучения

1…5 Вт вблизи и на расстоянии в несколько метров от датчика. Чем больше мощность передачи, тем с большего расстояния можно получить эффект. Радиоволны несколько ослабляются, но проходят сквозь стены. Они не «ослепляют» датчик, они только вызывают его срабатывание. Так можно спровоцировать серию ложных срабатываний, нажимая на кнопку «передача» в трансивере (в том числе портативной радиостанции), спрятанном в кармане, тем самым вызвать у обслуживающего персонала охраны желание отключить датчик или заменить его, то есть снять систему с охраны. Но воздействие радиоволнами не блокирует, а лишь дает «ложные» срабатывания, при этом PIR остается эффективен, и, если при непрерывном воздействие радиоволнами кто-то войдет в помещение, он выработает сигнал «тревога».

Если у специалиста имеется долговременный интерес к тому, как обезопасить оборудование и ценности под его охраной, рекомендую не ограничиваться консультациями и изучением новостей мира электроники (о таких вещах мало кто пишет, если только на специальных международных конференциях специалистов), а изучать, желательно практикой, уязвимые места PIR [2,3]. Тогда можно идти в ногу со злоумышленниками, а то и опережать, предупреждать их козни.

Но бывают случаи, когда в силу разных причин штатному специалисту «не до этого». Поэтому более ценится тот специалист, кто, помимо работы по инструкции, занимается еще и дополнительными исследованиями в теме и не равнодушен к работе. И такие люди во всем мире есть.

В России другая проблема. Заинтересованные люди с исследовательским интеллектом

есть, но нет желания и воли государства, а также и работодателя прислушиваться к их замечаниям и рекомендация. У нас государство и работодатель, как правило, поступает так, как инженер-установщик в Европе: по инструкции и не более.

Скажу честно: мне трудно общаться с людьми, которые все делают и мыслят по инструкции. Это очень плохо. В результате специалисты во всем мире понимают, что выявленные ими дефекты оборудования, идеи, рациональные предложения, исследования не нужны, и сами начинают работать только по инструкции. У небольших компаний, у которых нет широких возможностей исследовательских институтов, их штата и материальной базы, трудности только в том, чтобы практически (ситуативно) организовать воздействие на PIR различными другими системами и оборудованием. Зато, очевидно, исследуя проблематику комплексными методами, с привлечением когорты профильных специалистов, возможно получить и максимально полную картину, как еще можно нейтрализовать PIR сенсор (у нас его называют пироэлектрическим детектором). Для это разберемся в том, какова электронная логика работы современного ДД.

4.6. Логика работы схемы охранного датчика движения

В датчиках движения два управляемых канала, по которым идет сравнение поступающих входных сигналов. Логическая схема построена по принципам «И» и «ИЛИ». Логика работы таких ИК/РВ (СВЧ) датчиков по умолчанию на заводе-изготовителе, на любом уровне устанавливается: «И» – «ИЛИ».

Логика работы совмещенного ИК/РВ датчика, логика «И»: обнаружение проникновения ИК канала (1). «И» обнаружение (подтверждение) проникновения РВ (СВЧ) канала (2), при этом два канала работают одновременно. Другими словами, анализ сигналов СВЧ канала начинается после регистрации движения в ИК канале.

Логика работы совмещенного ИК/РВ датчика, логика «ИЛИ»: обнаружение проникновения ИК канала (1) – тревога, «ИЛИ» обнаружение проникновения РВ (СВЧ) канала (2) – тревога. Таким образом, обнаружение нарушения по любому каналу переводит датчик в режим тревоги.

Эта информация, по сути, общая для большинства фирм производителей, таких, как: Detectomat, Bosch, Digitize, Osbourne-Hoffman, AES-IntelliNet, Ademco, Visonic, Apollo, Watec,Computar, Commax, Fine, МГП Спецавтоматика, Ирсэт-Центр, Теко, Inter-M, Philips, Novar, Apollo,System Sensor, VESDA, Pyronix, ВЭРС, Legrand, НВП «Болид, Eff-Eff, «Сфера безопасности», ООО «СТД», НПО «Сибирский Арсенал», CROW, OPTEX, DSC, Inter M, «Бастион», ООО «Эпотос», ESA, Algorinet,TEXECOM, Grinnell, Viking, Chang, Der, Fire, Protections, Grundfos, Wilo, HILTI, Сталт, Спрут, НПГ «Гранит-Саламандра», НТК «Пламя», Артсок, НПО «Пожарная автоматика сервис», «Аргус-Спектр», «Импульс-ИВЦ», «Пожтехника МС», НПО «Пульс», НПФ «Сигма», «Тензор», «ИРСЭТ-Центр» Esmi, Aritech,Honeywell, Siemens, Securiton^

И даже этот список далеко не полон, ибо постоянно изменяется, появляются новые модели устройств.

4.7. Возможности и аспекты защиты магнитных датчиков, как уязвимого узла в системах охраны

Защита магнитных датчиков в электронных устройствах промышленного изготовления организована так. Для блокировки устройства применяется не один, а два магнито-контактных датчика, расположенных друг от друга на расстоянии примерно 15 мм и последовательно соединенных друг с другом. При этом нужно, чтобы у задающих элементов направления магнитных полей были встречными, взаимосвязанными. Тогда, при попытке саботирования работы датчиков внешним магнитом, один из задающих элементов поменяет направление магнитного поля, и переключит систему датчиков из режима «охрана» в режим

«тревога». Таким образом, злоумышленнику не удастся нейтрализовать систему охраны.

Практика обслуживания и проблемные вопросы

«Обойти» геркон действительно можно. К примеру, с помощью магнита, хотя проще замкнуть контакты геркона. Нередко между шлейфом и СМК (магнитным контактором) стоит КС (коробка соединительная). Не все монтажные организации делают дубляж СМК, не только от лени своей, но и для удешевления проекта. Оно и понятно: когда утверждена смета на 200–300 дверей, которые надо перекрыть СМК, вырастает приличная сумма, а когда есть ограничения в бюджете работ, приходится экономить, но это скорее вопрос частного порядка. А с другой стороны, какой смысл обходить геркон, когда он как правило идет одним шлейфом с ИК или РВ датчиком. Посему гораздо правильнее говорить о том, как обойти сам шлейф охраны.

Замечено, что даже у проверенных временем, хороших ИК-детекторов есть недостатки. ИК-датчик «Фотон 9» не реагирует на передвигающийся объект (человека), которого полностью закрывает тонированное в «цвет йода» стекло. ДД в этом случае не реагирует и, по сути, является бесполезным. Эксперимент с тонированным стеклом заинтересованные лица повторили несколько раз, сняли видео и отправили с сопроводительным письмом-претензией производителю.

Кроме того, недостатки имеют не только датчики типа «Фотон». А эксперимент можно подтвердить не только с помощью тонированного стекла (и даже не тонированного, но закрывающего человека целиком). В этот перечень входит и металлизированный материал (ткань). Как это объяснить, спросит заинтересованный читатель?

Допустим, что вы (объект, передвигающийся в зоне ответственности включенного ДД) попали в зону обнаружения, но стекло, расположенное между объектом (вами) и ИК датчиком, послужило блокировкой, а для чувствительной сенсорной секции ДД, за стеклом образовалась «мертвая» зона (в которой вы, как объект, и находились). Поскольку ИК датчик реагирует на изменяющуюся температуру (тепло) тела, а исходящее от вас тепло стекло просто отсекло (отражало) в обратную сторону, то есть обратно на вас; ведь стекло не пропускает тепло, как и многие другие теплозащитные материалы.

Конечно, не все так просто, но, ни один производитель не дает 100 % гарантии, что ИК ДД обеспечивают полную защиту охраняемой зоны. В этом смысле есть над чем задуматься.

Приложение
Практическое заключение экспертизы

1. Вводная часть

1.1. Основание для проведения экспертизы: Запрос компании Lenc от 30.03.2015 г. об инженерно-технологической экспертизе в части практических возможностей для принудительного вывода из строя пироэлектрического детектора (PIR) в системах охраны, сопряженных с датчиками движения.

1.2. Объект экспертизы: датчики движения в системах охраны

1.3. Место проведения экспертизы: Производственное помещение по адресу: г. Санкт-Петербург, Россия.

1.4. Эксперт: Кашкаров Андрей Петрович

Фабула обращения. Было несанкционированное проникновение в помещение, охраняемое устройством с PIR сенсором. При проникновении не поступил сигнал на пульт охраны (электронный модуль, взаимодействующий с PIR), отсюда предположение о том, что PIR сенсор не сработал. Такие случаи, возможно, имеют массовый характер в последние годы.

1.5. Вопросы, поставленные перед экспертизой:

1. Имеется ли возможность подавить PIR сенсор (установленный на стене помещения для горизонтального сканирования), вызвав его временную или постоянную неисправность, а также ситуацию, не характерную для нормальной эксплуатации вышеуказанного устройства?

2. Можно ли вызвать неисправность PIR посредством воздействия на него радиоволнами и (или) фотовспышкой?

3. С какого расстояния методом воздействия, указанным в п. 2, можно вывести из строя PIR?

4. Можно ли вызвать неисправность PIR посредством его ослепления ИК (спектр инфракрасного излучения) концентрированным лучом?

5. В случае, если у электронного устройства охраны на основе PIR, имеются недостатки, являются ли выявленные недостатки устранимыми?

6. В случае, если у электронного устройства охраны на основе PIR имеются недостатки, являются ли данные недостатки производственными либо эксплуатационными недостатками – связаны с ненадлежащей эксплуатацией, несоблюдением или ненадлежащем соблюдением Руководства по эксплуатации установки датчика охраны (или ненадлежащей установкой) технического обслуживания, вследствие нарушения правил хранения, вследствие действия третьих лиц, либо непреодолимой силы?

2. Исследовательская часть

2.1. Материально-технические средства (приборы, оборудование и пр.), применяемые при экспертизе:

• Портативная радиостанция (трансивер) Kenwood TH-F7E с передатчиком, действующим в рабочем диапазоном радиоволн 144–172 МГц и 430–446 МГц, и максимальной мощностью передатчика 5 Вт.

• HF transceiver – профессиональная радиостанция (трансивер) ICOM IC-718 с передатчиком, действующим в рабочем диапазоном радиоволн 1,8—28 МГц и максимальной мощностью 100 Вт.

• HF/VHF/UHF all mode transceiver – профессиональная радиостанция (трансивер) Yaesu FT897 с передатчиком, действующим (в частности) в рабочем диапазоном радиоволн 36–54 МГц и максимальной мощностью 50 Вт.

• Портативное устройство подавления сотовой связи и Wi-Fi типа TG-2000-121A.

• Краска быстросохнущая (нитро) черного цвета (спрей-баллон).

• Лак быстросохнущий для деревянных покрытий (спрей-баллон).

• Тряпка хлопчатобумажная (х/б), пропускающая солнечные лучи.

• Устройство с концентрированным лучом инфракрасного спектра излучения (длина волны 632,8 нм) мощностью 2 Вт.

• Инфракрасная внешняя подсветка (ИК-подсветка, с питанием 12 V DC) для установки на передний бампер в автомобиль – для улучшения качества видеофиксации (записи дорожной ситуации по ходу движения) в темное время суток.

• Цифровой тестер для контроля состояния шлейфа «выхода» датчика охраны.

• Цифровая фотокамера со вспышкой «Olympus E420».

2.2. Нормативная и справочная документация

2.2.1. ГОСТ 24444—87 Оборудование технологическое. Общие требования монтажной технологии.

2.2.2. ГОСТ 26433.1—89 Правила выполнения измерений. Элементы заводского исполнения.

2.3. Методы исследования

2.3.1. Органолептический-визуальный. Суть метода состоит в осмотре оборудования в целом и его составных частей при естественном и искусственном освещении, в том числе с разбором корпуса отдельного (локального) датчика движения для систем охраны.

2.3.2. Измерительный. Суть метода состоит в проведении необходимых экспериментов (воздействия на рабочую зону PIR сенсора различными приспособлениями и устройствами, указанными в п. 2.1), замеров в соответствии с правилами ГОСТ 26433.1—89 «Правила выполнения измерений. Элементы заводского исполнения».

А также краш-тест без всяких правил в экспериментальном порядке комплексного воздействия.

2.4. Объект исследования, описание

Датчик системы охраны (далее в тексте – выносной датчик) = «извещатель охранный» – это электронное устройство на основе PIR типа «Орлан», «Фотон» и аналогичный. Особенность датчика в том, что он рассчитан на подключение в систему охраны (является элементом шлейфа единой системы), обладает двумя контрольными функциями – чувствительностью к акустическому фону охраняемого помещения (см. отверстие для микрофона на корпусе датчика) и чувствительностью к изменению инфракрасного (теплового) фона в охраняемой зоне благодаря линзе Френеля. Питание датчика + 12 V DC ±20 %. Выходной сигнал передается к модулю системы охраны по проводам (двухпроводная линия).

В принципе охранные датчики движения имеют одинаковый принцип действия и различаются некоторыми дополнительными функциями, к примеру, световой и звуковой индикацией срабатывания (выработки сигнала «тревога») и регулировкой чувствительности.

На рис. 4.4 представлено устройство ИО315-1 «Орлан» (производитель-экспортер «Риэлта») для цифрового кодированного охранного комплекса типа «Сигнал-201» и аналогичных. Внешне он выглядит как коробочка с выпуклым матовым стеклом, обращенным к зоне охраны. «Матовое стекло» неоднородно, а разграничено на сектора с разным углом наклона и плотности относительно поверхности. Это линзы Френеля. Известный французский изобретатель Френель знаменит тем, что в начале XX в. предложил и воплотил в реальность проект оборудования маяков специальными выпуклыми стеклами неоднородного состава: стекла состояли из нескольких частей, наклоненных под разным углом относительно друг друга. Свет, пропущенный через такие линзы, проникает сквозь туман на много морских миль.

Важно понимать, что в зависимости от типа применяемой линзы можно получать территорию перекрытия (охраны) датчика вертикальную – типа «занавес», широкую по глубине, сфокусированную или размытую. Когда в зоне защиты появляется излучатель тепла – человек или животное – изменение теплового излучения в инфракрасном спектре улавливается PIR, сигнал преобразовывается в электрический ток, усиливается до необходимого уровня (электрический КПОП-уровень). Так в выносных и локальных датчиках охранных систем вырабатывается сигнал «тревога».

Датчик снабжен трехуровневым светодиодным индикатором срабатывания и регулировкой чувствительности зоны сканирования. Это позволяет визуально контролировать (издалека), сколько уровней чувствительности уже активно. К примеру, при появлении в зоне мониторинга мыши загорится только один индикатор, при появлении человека средней комплекции – все три. В какой момент будет выработан электрический сигнал «тревога» для охранной системы – зависит от установки чувствительности прибора. Она осуществляется с помощью тонкой монтажной отвертки (поворотом движка подстроечного резистора на печатной плате устройства – для этого корпус должен быть вскрыт). Были случаи, когда летом датчик работал отлично, зимой самопроизвольно давал сигнал «тревоги». Выяснили, что реагирует на теплый воздух, поднимающийся от батареи. Но ложные сигналы тревоги не суть эксперимента, мы рассматриваем возможности блокировать датчики на основе PIR, поэтому пойдем дальше.

Почти все современные датчики движения (присутствия) на сегодня – это датчики с круговыми или овальными диаграммами обнаружения. Поэтому охватить прямоугольное помещение датчиками с круговыми диаграммами можно только с перехлестом диаграмм. Вроде бы немецкая компания Theben AG (возможно, кто-то еще) делает датчики присутствия

с квадратной зоной обнаружения, что значительно упрощает проектирование. В этом случае датчиков требуется меньше: четыре «квадратных» вместо семи с круговой диаграммой. В таком варианте углы помещения надежно перекрываются.

Как работает датчик движения? По своей физической природе видимый свет и ИК (инфракрасное) излучение одинаковы. ИК излучение можно сфокусировать линзой, как и обычный свет. При попадании ИК излучения на фотоэлемент особого состава, он меняет свои параметры. При комнатной температуре в видимом свете тела людей «не светятся», а в ИК диапазоне – просто «сияют». Все это хорошо иллюстрируют такие устройства, как тепловизоры. Яркость ИК излучения зависит от температуры тела; что горячее – светится ярче, что холоднее – светится слабее.

Контраст между ИК свечением человека и ИК свечением холодного окна – значительный. С другой стороны, ИК свет человека и ИК свет теплого пола (газовой или тепловой плиты, иных источников тепла) практически одинаковы, поэтому распознать человека на фоне теплого пола почти невозможно. И это обстоятельство в дальнейшем рассуждении и выводах данной экспертизы будет иметь ключевое значение. Рассматриваемые датчики реагируют на появление и исчезновение ИК света на специальном пироэлектрическом детекторе (элементе). Появление и исчезновение ИК света вызвано активной деятельностью человека, реже факторами, не связанными с человеком, к примеру, движением теплого воздуха от батареи.

Белое матовое стекло (см. рис. 4.4 и 4.5, фото слева – на самом деле пластик) – мультилинза Френеля – состоит из нескольких (чем больше – тем надежнее система охраны) маленьких линз, каждая из которых фокусирует проникающие ИК потоки на плоскость PIR сенсора, а одна из них – непосредственно на сам фотоэлемент (так сигнал регистрируется). Если объект движется, то через какое-то время фокус линзы уходит с фотоэлемента PIR и сигнал пропадает. Затем (спустя миллисекунду) уже другая линза фокусирует ИК поток человека на фотоэлемент – сигнал опять появляется. Такое появление-исчезновение-появление сигнала – признак присутствия человека. Каждая линза охватывает свой сегмент. Сигнал пропадает при выходе человека (руки человека) за границы этого сегмента. При перемещении внутри сегмента сигнал не меняется. Чем больше таких линз, тем более мелкие движения может улавливать датчик.

При удалении объекта от датчика размер сегмента увеличивается и с какого-то расстояния все мелкие движения, к примеру, движение рук, покачивания головы будут находиться в границах одного сегмента. После этого расстояния датчик присутствия может работать уже только как датчик движения (реагировать только на очень «широкие» движения объекта). А у бытовых датчиков движения сегменты более крупные по сравнению с датчиками присутствия, применяемых в охранных системах. Датчики движения «загрублены» и реагируют на более сильный ИК-поток по сравнению с датчиками присутствия.

При рассмотрении конкретного датчика замечу, что он также имеет функцию самоохраны – для этого предусмотрена кнопка SA2, контакты которой замкнуты при нормально закрытой крышке корпуса – для того, чтобы не было несанкционированного (не зафиксированного) вскрытия корпуса датчика системы охраны. Переключатель с обозначением SA1 отвечает за чувствительность датчика и комбинацию выходных сигналов при срабатывании шлейфа охраны. Подключение производится к клеммнику на плате датчика. Все эти особенности могут несколько отличаться, если применяется датчик другой модели. Однако тип и принцип действия одинаков для всех локальных выносных датчиков на основе PIR для охранных систем.

2.4.1. Уточнение перед исследованием. Смысловые понятия и определения, которые будут использованы в экспертном заключении.

PIR sensor = пироэлектрический детектор = PIR = чувствительный к ИК спектру излучения радиоэлектронный элемент типа RE46 (и аналогичный).

Датчик системы охраны (далее в тексте – выносной датчик) = «извещатель

охранный» – это электронное устройство на основе PIR типа «Орлан» и аналогичный.

2.4.2. Приложение: фото в электронном виде внешнего вида датчика системы охраны и его печатной платы с чувствительным элементом RE46.

2.5. Результаты исследований

2.5.1. Представленная на экспертизу документация

Оборудование, сопутствующие документы, дефектные ведомости, особенности установки оборудования, иные подробности дела, кроме описанных выше, – в фабуле дела, на экспертизу не представлены

2.5.2. Внешний осмотр оборудования

2.5.2.1. Выносной охранный датчик типа «Орлан» расположен в сухом производственном помещении, установлен вертикально в помещении с площадью 35 м2, подключен к системе электропитания, выход датчика (двухпроводный электрический шлейф подключен к индикатору – мультиметру (тестеру) для контроля состоянии срабатывания датчика по мере экспериментальных воздействий.

2.5.2.2. Оборудование представляет собой датчик движения (ДД) для установки внутри помещений, ни одна современная система охраны сегодня не обойдется без этих датчиков, относительно недорогих и доступных. Они предназначены для устройств охранных сигнализаций и безопасности, предупреждения и индикации присутствия посредством передачи электрического сигнала по шлейфу охраны (по двухпроводной линии) к центральному модулю.

Причем в данном случае срабатывание (сигнал «тревога») происходит от двух причин: нарушение акустического фона (выносной датчик по техническим и конструктивным особенностям, связанным с применением электретного микрофона реагирует на резкий звук, стук, хлопок, а не «мягкое» пение «колыбельной»; реагирует на расстоянии до 3 м (от датчика) на звук силой не ниже 45 дБ, более слабый звук не приведет к выработке сигнала «тревога»).

Но надо также понимать, что не все модели датчиков для систем охраны снабжены «звуковым контролем-мониторингом помещения». Хотя «двойной контроль» (как будет видно из дальнейшего рассуждения) делает такие устройства более надежными. И вторая причина – при резком изменении «теплового» фона контролируемого помещения, то есть при движении в зоне ответственности датчика некоего теплового объекта. Этим объектом может быть даже мышь.

Датчик имеет многоуровневую систему настройки чувствительности, реализованную с помощью электронных элементов и корректируемую (при желании). Это является одним из аспектов необходимости периодического контроля подобных датчиков (регламентных работ) на работоспособность теми, кто их применяет. Дело в том, что почти любое электронное устройство бытового или «гражданского» назначение (в отличие от так называемой «военной приемки») подвержено влиянию температуры окружающего воздуха, а охранные датчики на основе PIR еще и подвержены оседанию пыли на внешней поверхности линзы Френеля (белое матовое на фото 1 слева), на внутренней ее поверхности и непосредственно на рабочей поверхности самого сенсора PIR. Во время работы в режиме 24 часа радиоэлементы устройства незначительно нагреваются (выше комнатной температуры) и таким образом, выделяют тепло. Это привлекает в их корпуса насекомых.

В практике бывают случаи, когда между линзой Френеля и рабочей поверхностью PIR в корпусе датчика движения находили «заснувших» муху или таракана. Что, разумеется, делало такой датчик практически бесполезным, то есть «слепым» даже и без несанкционированного воздействия злоумышленников. Чтобы этого не происходило надо следить за санитарной обработкой помещения.

Таким образом, датчик охраны может быть лишен всех своих преимуществ по причине оседании пыли (даже незначительно) на рабочей поверхности своего главного элемента PIR (внутри корпуса устройства), а также на внутренней и (или) внешней поверхности линзы Френеля, либо нахождения внутри корпуса устройства насекомых и иных посторонних

предметов.

Вот почему надо признать заблуждением субъективное мнение о том, что такие датчики не требуют обслуживания. Необходимо (в зависимости от условий эксплуатации и конкретики помещения) не реже одного раза в полгода открывать корпус датчика, осматривать его запыление и при необходимости протирать мягкой сухой тряпочкой (желательно фланель) поверхность линзы Френеля с внешней и внутренней стороны. Такие, кажущиеся простыми, методы обслуживания добавят надежности всей охранной системе, работающей с PIR.

Как один из предварительных советов можно рекомендовать такой: кроме периодической визуальной проверки (внешне и внутренне) корпусов датчиков движения, особенно в помещениях с нестабильной температурной обстановкой, где возможно появление и оседание пыли (в том числе после проводимых невдалеке строительных работ), необходимо после постановки в режим охрана всей системы сделать «обход» и проверить помещение (я) на ложное срабатывание, а уже затем устанавливать систему в режим охраны и покидать объект. К сожалению, такая мера также остается актуальной.

Рассматриваемые датчики рассчитаны для совместной работы в системах с централизованным питанием и резервными источниками бесперебойного питания (ИБП) – в многофункциональных системах управления охранным комплексом, кодовым доступом, индикацией и дистанционным управлением.

Потеря чувствительности выносного датчика может быть связана с изменением (самопроизвольным) настроек чувствительности; весьма частый случай в практике такого обоснования – колебание температурного климата в охраняемом помещении. К примеру, если охранная система установлена в холодный период года в музее, который топят по утрам, то уже к позднему вечеру тепловой (температурный) фон изменяется, что корректирует чувствительность датчика.

То же можно ожидать при несанкционированной и (или) принудительной аварии в системе отопления помещения, которая накануне проникновения в него привела к локальной потере чувствительности датчиков движения. При понижении температуры чувствительность таких датчиков снижается. Можно вывести график падения чувствительности на примере конкретной модели (зависимость падения чувствительность к ИК фону от температуры окружающей среды), однако такой вопрос пока не поставлен заказчиком.

Должен заметить, что потеря чувствительности почти не связана с колебаниями напряжения питания охранной системы (при условии, что колебания в пределах допустимой нормы) и при отключении питания по любым причинам произойдет срабатывание датчика (выработка сигнала «тревога»), а не его «ослепление» или «бесполезность». В этом ключе необходимо понимать особенность передачи сигнала «тревога» на центральный модуль охраны (который – по конкретным индивидуальным характеристикам модели – может получать и обрабатывать сигналы от нескольких десятков таких датчиков). При «нормальной» штатной работе датчика охранной системы его «выход» представляет собой замкнутую электрическую цепь, при выработке сигнала «тревога» цепь размыкается. Также она размыкается при нарушении шлейфа проводной связи датчика и основного модуля охраны, а также при аварии в системе электропитания. Поэтому всех этих случаев следует опасаться меньше всего: при таких условиях датчик скорее даст ложный сигнал тревоги, чем окажется «выключенным» и бесполезным.

2.5.3. Реальные эксперименты для обоснования выводов экспертного заключения.

Для проверки на функционирование устройство было установлено на стене рабочей производственной площадки площадью 35 м2 на расстоянии (высоте) 2 м от пола. Такая установка (не менее 1,8 м от нижней границы помещения рекомендована производителем и ее следует соблюдать). Линза Френеля обращена к двери в помещение, которая закрыта. Подключено питание. К выходу датчика подключен тестер-индикатор состояния (сам тестер выведен в соседнее помещение, за стеной, чтобы не было влияние на чистоту эксперимента и

можно было бы свободно наблюдать за показаниями прибора, не находясь в зоне ответственности испытуемого датчика). Контакты на выходе датчика нормально замкнуты. Регулировка чувствительность выведена в среднее положение.

Эксперимент 1
Простое закрытие рабочей зоны

При накрывании линзы Френеля прозрачной тряпкой датчик теряет чувствительность. Даже манипуляции руками перед внешней поверхностью линзы Френеля не дают эффекта срабатывания. Это «эффект попугая». Когда клетку с разговорчивым попугаем накрывают платком, попугай, хоть и не закрывает глаз, но замолкает. Таким образом, сделать датчик охраны временно бесполезным можно простым накрытием его рабочей поверхности любой тряпкой. В продолжении эксперимента были предприняты попытки закрашивания рабочей поверхности датчика охраны из распылителя быстросохнущей (нитро) краской черного цвета (спрей-баллон) и спрея быстросохнущего, но прозрачного лака. Эффект тот же «ослепленный» датчик полностью перестает контролировать зону «ответственности».

Другое дело, что надо исхитриться и как-то суметь подобраться к включенному датчику, установленному на стене, ведь зайти с фронта нельзя – это вызовет срабатывание. Значит, остается один путь – опустить тряпку сверху (с потолка или со стороны стены – с тыльной стороны датчика).

Рекомендация: обезопасить стены, потолок – подходы к датчику со стороны «слепых» зон, что можно сделать установкой нескольких датчиков в одном помещении – с перекрестными зонами мониторинга.

Стоимость данной работы по дополнительной безопасности зависит от производственных возможностей организации, осуществляющей техническое обслуживание данного оборудования.

Эксперимент 2
Воздействие с помощью радиоволн

В этом эксперименте было проведено последовательное воздействие радиоволнами разной частоты и мощности посредством поочередного включения трансиверов (см. п. 2.1) на передачу. Во всех случаях воздействие вызывало немедленное однократное (не продолжительное) срабатывание датчика охраны.

Таким образом, не зависимо от модуляции радиоволн, их частоты (последовательно применялись попытки радиопередачи из соседней комнаты на частотах 1,8 МГц, 3,5 МГц, 14 МГц, 27,5 МГц, 36,5 МГц, 145,5 МГц, 172,0 МГц, 435,0 МГц, 446, 6 МГц) датчик срабатывал каждый раз, значит при попытках такого несанкционированного воздействия он скорее даст серию ложных срабатываний, чем останется бесполезно-заблокированным злоумышленниками.

Здесь следует отметить, что сделаны практические попытки воздействия на датчик на радиочастотах, передатчики для которых наиболее популярны и могут быть доступны в открытом доступе. Однако, следующим шагом было проверена реакция датчика на входящий звонок сотового телефона стандарта GSM с частотным диапазоном 900/1800 МГц. При входящем и исходящих звонках из соседней комнаты датчик не никак реагировал (при прохождении звонка и ведении разговора по сотовому телефону и входе в охраняемое помещение датчик нормально срабатывал).

Но при расположении сотового телефона на расстоянии 1 метр от корпуса датчика и организации входящего звонка на телефон происходило срабатывание и выработка сигнала «тревога» в штатном режиме. После воздействия на частотах сотовой связи датчик также срабатывал нормально.

Эксперимент 3
Воздействие с помощью устройства, заглушающего радиосвязь на частотах 900/1800/2400 мГц (включая связь по протоколу 802 Wi-Fi)

При всех трех режимах, включая высокочастотный 2,4 ГГц, датчик вел себя так же, как в эксперименте 2. При включении устройства подавления (генератора заглушки см. п. 2.1.) на расстоянии до 30 метров фиксировалось самопроизвольное однократное срабатывание датчика охраны на основе PIR. После того, как датчик возвращался в режим охраны помещения (но воздействие генератора заглушки не прерывалось) он в штатном режиме срабатывал при появлении в зоне мониторинга человека (при входе в охраняемую комнату).

Рекомендации по экспериментам 2 и 3: с этой стороны датчик вполне стабилен и устойчив, скорее можно ожидать ложные срабатывания, чем его дистанционную блокировку. По крайней мере в данном случае – для последней опасений не выявлено.

Эксперимент 4
Воздействие пучком лучей и ИК подсветкой

С разного расстояния от рабочей поверхности датчика (вариативно) применено устройство с концентрированным лучом инфракрасного спектра излучения красного цвет на основе полупроводников из арсенида галлия. Если направить лучи с близкого расстояния 80—100 см от линзы Френеля, удается заблокировать датчик в 10 из 15-ти случаев такого воздействия. Однако в этом эксперименте надо понимать, что я имел возможность использовать только относительно маломощный концентрированный световой луч, с длиной волны в диапазоне 632,8 нм (нанометров), имеющий лишь подобие лазера (если предполагать, что лазер имеет не обывательское, а научно обоснованное определение).

Таким образом, детские игрушки-указки еще с меньшей мощностью в несколько мВт вообще нельзя считать лазерами. Такие «лазерные указки», которые, впрочем, вполне реально подсвечивают объекты на расстоянии до 200 м с сохранением приемлемой концентрации (фокусировки) светового пучка, на мой взгляд, не способны нейтрализовать датчик с PIR. Если даже более мощная система делает это не стабильно. Этим объясняется нестабильность результатов их применения и их вариативность.

С дальнего расстояния в 4,5 метра (расстояние от входа в помещение до датчика охраны) заблокировать («ослепить») датчик таким экспериментом с моим оборудованием не удалось. Однако можно догадываться (предполагать), что у людей, злоупотребляющих правилами, имеющих больший дар соображения и средства к покупке мощных лазерных (bild) устройств, это могло получиться лучше, чем у меня.

Даже на основании простого эксперимента очевидно, что датчик охраны, как минимум, ведет себя нестабильно при воздействии световым потоком с длиной волны (красного спектра) 632,8 нм на внешнюю поверхность линзы Френеля, в то время как при разобранном корпусе датчика (вторая часть эксперимента 4) и прямом воздействии лучами на рабочую поверхность PIR сенсора он стабильно «ослепляется», то есть устройство не вырабатывает сигнал «тревоги».

Но важно и то, что сам по себе PIR сенсор, как радиоэлектронный элемент, реализованный в корпусе RE46 и аналогичном, без линзы Френеля, не является достаточным для датчика охранной сигнализации, и даже без намеренного воздействия ИК лучами и (или) лазером на его рабочую поверхность (без линзы Френеля) не дает срабатываний при движении людей в зоне мониторинга, и даже при манипуляции руками с близкого расстояния (0,5 м). Поэтому с полной гарантией сказать о том, что пучком лучей с длиной волны 632 нм можно гарантировано «ослепить» датчик охраны, нельзя. Но можно утверждать, что таким воздействием датчик приводится в нестабильное рабочее состояние, а при использовании более мощных устройств воздействия и (или bild, лазеров) полностью блокируется.

К примеру, в свободном доступе есть мощные «лазерные устройства» (на самом деле – это не лазеры по определению, но их некое подобие). При заявленной (никто не проверял) мощности 2 Вт и длине волны 532 нм (зеленый спектр излучения) или длиной волны 360…480 нм (голубой спектр) с линейной поляризацией (50: 1) и сфокусированном световом пучке (диаметр луча) 1,2 мм, такой луч может быть очень эффективным для блокировки датчиков охраны на основе PIR. За последние 15 лет в производстве светодиодов достигнут значительный прогресс, рынок энергоэффективного освещения расширился, и такие устройства можно купить. Как вариант можно обратить внимание на фонари типа Nightsun с силой света 50 000 Лм и углом расхождения луча менее 0,5°, IMAX-проекторы и прочее оборудование, предварительно его испытав.

Еще более интересной представляется другая часть эксперимента, когда на тот же датчик воздействовали ИК лучами от обычного пульта дистанционного управления (ПДУ) бытовой радиоаппаратуры. Как известно, при нажатии на кнопку ПДУ светодиод излучает невидимый человеческому глазу световой спектр. Причем излучает не постоянно, а импульсно и последовательность импульсов (пачек импульсов) определяется тем, какая именно кнопка нажата.

Так происходит дистанционное управление ИК лучами в бытовой (и иной) радиоаппаратуре. Если же подключить мощный ИК-диод (блок ИК диодов) к источнику питания постоянно, без схемы генератора ВЧ импульсов, то такой инфракрасный фон теоретически может служить причиной для восприятия его PIR-сенсором и. блокирования самого себя.

В рамках эксперимента я применил блок относительно мощной (10 Вт) ИК подсветки, предназначенный для устройств автомобильных видеорегистраторов. Блок дополнительно устанавливается перед решеткой радиатора автомобиля и направлен по ходу движения, тогда автомобильный видеорегистратор, установленный в салоне, лучше «видит» в ночное время пространство перед собой, и, соответственно, качество видеофиксации в разы повышается, тем не менее самого света излучения ИК спектра люди почти не видят; едва-едва «покраснение» излучающих диодов видно в полной темноте. Это устройство было применено мною в эксперименте и с расстояния в 2 м оно блокировало датчик охраны следующим образом. При первом включении (дистанционно, люди из помещения вышли) датчик однократно сработал, среагировав на внезапно возникший сильный ИК фон в зоне мониторинга, а затем (ИК подсветка не выключалась) уже больше не реагировал ни на что.

Таким образом, воздействие ИК лучами вполне блокирует датчик. Только для гарантированного эффекта оно должно быть еще большей мощности, чем применяемое мною в эксперименте. Кроме того, для блокировки датчика требуется, как вариант, его пронести в помещение (установить в соседнем) и запустить не в момент проникновения (и не перед ним), а при скоплении народа в рабочее время.

Мощный источник ИК излучения мог бы заблокировать не один, а несколько датчиков на основе PIR сенсоров в нескольких соседних помещениях (масштаб в зависимости от мощности).

Ослепление PIR с помощью сконцентрированных лучей (с длиной волны, приближенной к чувствительному спектру PIR) и bild, а также с помощью ПДУ и – особенно – ИК подсветки различного назначения возможно. Для подтверждения и устранения данного дефекта требуется дальнейшая диагностика системы.

Тот, кто успешно уже применял эту систему, должен был, во-первых, задуматься обо всем здесь написанном, а во-вторых, заранее подготовиться: установить – какие именно модели датчиков охраны и в целом система используется, поэкспериментировать с ней дома, и получив апробацию своей идее – реализовать ее на практике.

При оперативных разработках, ежели предполагать, что они кому-то были бы нужны в конкретной ситуации, надо бы посмотреть, кто за некоторое время заходил в помещение и интересовался оборудованием, хотя бы визуально. В этом может помочь видеосъемка.

Эксперимент 5
Воздействие фотовспышкой

В эксперименте принимала участие цифровая фотокамера со вспышкой «Olympus E-420». Фотокамера последовательно устанавливалась в режим единичной фотовспышки и скоростной съемки, когда фотовспышка срабатывала с периодичностью 5 раз в секунду. При попытке «ослепления» датчика с расстояния 4,5 м эффект отрицательный. Датчик работал в штатном режиме и реагировал выработкой сигнала «тревога» на входившего в следующую секунду человека. При воздействии фотовспышкой с расстояния 0,7 м (перед линзой Френеля) датчик действительно удавалось «заблокировать», и он не вырабатывал сигнал «тревога» в последующие несколько секунд.

Тем не менее, уже при следующем заходе в комнату (спустя 5 секунд) датчик дал сигнал «тревога».

Однако этот способ блокировки сопряжен с некоторыми трудностями. Во-первых, имея лишь обычное бытовое оборудование в виде фотокамеры со вспышкой, требуется близко (и незаметно) подобраться к датчику, что почти невозможно, либо ослепить его с близкого расстояния со стороны потолка (но для этого нужен подход и оттуда). Во-вторых, такой метод не гарантирует 100 % блокировки датчика охраны, а лишь дает шанс его ослепить.

Впрочем, ранее при экспериментах с бытовыми датчиками движения, которые были сопряжены не с охранными системами, а с устройствами управлениями силовыми электрическими цепями (то есть имели не специализированное, а бытовое предназначение, хотя принцип работы PIR един) в осветительной сети 220 В (управляли освещением), мне удавалось с одного раза так ослепить датчик, что он потом больше уже не работал до тех пор, пока с него полностью не снимали (отключали) питание, а спустя некоторое время 3.. 10 минут, вновь не подавали его на устройство.

На момент проведения экспертизы проверить блокировку всех возможных датчиков не представляется возможным, поэтому данная экспертиза не может подтвердить или опровергнуть наличие указанного дефекта.

Рекомендации: с большой долей вероятности можно говорить о том, что «ослепление» датчика охраны с помощью обычной фотовспышки – для его блокировки на длительное время – не эффективно. Кроме того, перекрестный мониторинг помещения с помощью нескольких датчиков позволит обеспечить более надежную защиту систему.

Эксперимент 6
Частое отключение питания по нескольку десятков раз в минуту

На практике замечено, что датчики на основе PIR могут стать бесполезными (не вырабатывать сигнала «тревога») при перебоях в электроснабжении. К примеру, вывести из строя такой датчик можно даже дистанционно, по несколько десятков раз за одну минуту (принудительно) включая и отключая его питание.

Нельзя сказать в точности – в какой момент проявится «триггерный эффект», но он, как правило, проявляется одним и тем же симптомом: датчик перестает реагировать на перемещение в охраняемой зоне.

В условиях хорошо отлаженного (резервного) и защищенного электроснабжения такая ситуация маловероятна. Но иметь ее в виду следует.

3. Ответы на вопросы экспертизы

Вопрос 1. С какого расстояния методом воздействия, указанным в п. 2 (предыдущий абзац), можно вывести из строя PIR?

Фотовспышкой обычной бытовой фотокамеры – с расстояния 0,7 метра и ближе. И

даже этот эффект не гарантирован.

Вопрос 2. В случае, если у электронного устройства охраны на основе PIR, имеются недостатки, являются ли выявленные недостатки устранимыми?

С учетом навыков рядового сотрудника технической службы охраны на месте устранить возможность блокировки датчиков охраны на основе PIR весьма сложно. Необходима проработка (исследования, испытания) защиты датчиков от ослепления направленным воздействием ИК-лучами (мощной установки) путем подбора специальных линз.

Не уповая на разрекламированные свойства датчиков охраны на основе PIR сенсоров необходима дополнительная комплексная защита помещения, как то посредством установки датчиков для перекрестного мониторинга территории, а еще лучше – путем установки разного типа датчиков – как PIR сенсоров, так и других систем охраны, и чем менее эти системы будут популярны (серийное производство), тем лучше; речь идет об индивидуальных системах, разработанных малым «тиражом», под конкретную задачу и смонтированных специалистами одной подконтрольной компании, для устранения утечки информации.

Вопрос 3. В случае, если у электронного устройства охраны на основе PIR имеются недостатки, являются ли данные недостатки производственными либо эксплуатационными, связанными с ненадлежащей эксплуатацией, ненадлежащим соблюдением руководства по установке датчика охраны, технического обслуживания, вследствие нарушения правил хранения, вследствие действия третьих лиц, либо непреодолимой силы)?

У электронных устройств охраны на основе PIR, разумеется, имеются недостатки. При соблюдении технических требований к установке датчиков в помещении (высота, температурный режим, влажность, требования к электропитанию, проводке – ее длине, антивандаль-ной защите, и др.) все выявленные недостатки надо принять как данность. Отчасти вследствие некачественного (недостаточного) регламентного обслуживания (которое почти нигде не производится) могут выявляться проблемы, приводящие к неэффективности системы охраны (см. раздел 2.5). Действия третьих лиц и непреодолимой силы необходимо, по возможности, предусматривать в связи с данным выше обзором и рекомендациями.

Мнение вне поставленных вопросов

Датчик движения реагирует на перемещение в своей зоне контроля предметов, излучающих тепло. Это могут быть люди и животные. Изменение ИК фона вызывает движение, как человека, так и любых нагретых объектов (животные, поток теплого воздуха).

Датчик движения, установленный на кухне (или в иных помещениях), где находится газовая плита, может вести себя неадекватно, демонстрируя сбой в работе. Таким образом, для нейтрализации датчика надо создать устойчивую (стабильную) ситуацию постоянного теплового фона в помещении с помощью источника теплового фона большой мощности.

Кроме постоянного воздействия лазером или пучком (поток) ИК излучения, вблизи рабочей поверхности датчика может быть установлена локальная газовая горелка (к примеру) или устройство со сходным принципом излучения. В этом случае PIR сенсор воспримет тепловой фон как норму и «не заметит» движение вдали.

Литература, информация

1. Bishop Fox, Drew Porter (Black hat USA-2013, 27 juli – 1 august, 2013, Las Vegas); http://www.blackhat.com/ us-13/speakers/Drew– Porter.html

2. Black hat USA-2014 (2–7 august, 2014, Las Vegas); http:// www.blackhat.com/us-14/

3. Black hat mobile security summit London-2015; https:// www.blackhat.com/ldn-15/

4. *Кашкаров А.П.* 500 схем для радиолюбителей. Электронные датчики. – СПб.: Наука и Техника, 2007.

5. *Кашкаров А.П.* Современные сигнализации для дома, автомобиля, самостоятельного творчества. – М.: ДМК-Пресс, 2014.

6. *Кашкаров А.П.* Справочно-практическое пособие электрика. – Ростов н/Д: Феникс, 2011.