***А.В. ТЕЛЬНЫЙ,*** к.т.н., доцент кафедры ИЗИ
***Ю.В.КУЛЯШ*** студент группы КЗИ108

# СПОСОБЫ ОБХОДА ОХРАННЫХ ИЗВЕЩАТЕЛЕЙ И ПРИЕМО-КОНТРОЛЬНЫХ ПРИБОРОВ (ПКП) И РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ОТ ВОЗМОЖНЫХ ПОПЫТОК ПРЕОДОЛЕНИЯ ОХРАННОЙ СИГНАЛИЗАЦИИ

Статья посвящена способам обхода охранных извещателей. С учетом развития технологий многие способы обхода могут или уже стали неактуальными, но их применимость может сохраниться для бюджетных решений и в будущем. Статья не претендует на полноту изложения в связи со спецификой тематики.

Ключевые слова: охранные извещатели, приемно-контрольные приборы; срабатывание извещателя; предотвращение проникновения.

Основная задача любого охранного извещателя – это обнаружение проникновения в охраняемое помещение (территорию) с последующей подачей тревожного извещения (звукового, светового, сообщение на пульт охраны и т. п.). Один из способов недопущения реакции на сообщение – вывести из строя или канал, по которому будет передаваться сообщение, или само устройство формирование тревожного извещения (извещателя). В данной статье не рассматривается такого типа способы блокирования извещателя.

Функционирование любого типа извещателя основано на показаниях датчика определенного физического принципа действия. Датчик контролирует определенный параметр среды, при изменении которого происходит срабатывание извещателя. Если не допустить изменение такого параметра, то возможно беспрепятственный обход извещателя. Именно такие способы и рассматриваются в данной статье. Следует знать, что в действительности контролируемый параметр не является постоянной величиной и в течение определенных временных промежутков изменяется в допустимом диапазоне. Такой диапазон определяется как чувствительностью извещателя, так и подстраиваемой аппаратной и программной компонентами самого извещателя. Большинство извещателей снабжены возможностью настройки, от которых может зависеть срабатывание извещателя. Неправильная настройка и установка извещателя может привести к ложным срабатываниям, а также к повышению вероятности несрабатывания. Следует учитывать также и допустимые для извещателя параметры окружающей среды. Периодически нужно проводит техническое обслуживание извещателя, для некоторых типов извещателей нужен и визуальный контроль.

**Универсальные методы предотвращения проникновения.**

а) Дополнительная установка извещателей другого принципа действия или использование совмещенных извещателей.

б) Маскировка извещателя и ПКП под окружающий интерьер и размещение его внутри конструкций.

в) Усложнение физического доступа к извещателю и ПКП, например, антивандальные короба, металлическая сетка, расположение значительнее выше человеческого роста и т. п.

## 2 Извещатели

### 2.1 Электроконтактные извещатели

а) Вырез в полотне или обрезка места установки извещателя

Для злоумышленника важно знать схему расположения проводника. С помощью угловой шлифовальной машины, дрели и других подобных инструментов выполняется резка

материала. Возможно, понадобиться фиксация фрагментов полотна для исключения возможности случайного разрыва проводника, а также размещение между проводниками изолятора. Расположение проводника в несколько слоев сделает данный метод почти невозможным. Прорезь в полотне выполняется по границе петли проводника.

б) Воздействие на соединительный клей (для ленточных проводников)

Этот способ применим к стеклу и, возможно, к металлу, но почти невозможен для других материалов. Суть заключается в последовательном нагреве и охлаждении участков, где приклеен проводник. За счет конденсации влаги и расширения/сужения клей должен потерять свои свойства, а лента отвалиться. Если применяется водостойкий клей, то такой способ невозможен.

Следует использовать рекомендованные средства монтажа, которые обычно указываются в инструкции к оборудованию. Также необходимо регулярно обследовать состояние извещателя.

в) Включение в цепь удлиняющего проводника, разрыв имеющейся

Если не учитывается сопротивление проводника или при не полном использовании ленты, возможно припайка петли и последующий разрыв между контактами петли.

Данный способ невозможен, если нет физического доступа к проводнику.

**2.2 Магнитоконтактные извещатели**

а) Вставка постороннего магнита. Для этого способа необходим физический доступ к извещателю. При этом магнит, который подключается, заменяет часть извещателя не подключенную к шлейфу. Знание модели извещателя поможет злоумышленнику подобрать соответствующий магнит. При этом необходимо пространство для вставки своего магнита. При установке и настройке допускается некоторое расстояние между составными частями извещателя, это расстояние может быть использовано злоумышленником.

Следует маскировать извещатель, а также максимально снизить амплитуду колебания подвижной части (двери, створки окна и т. п.) в закрытом положении. Также, возможно, поможет экранирование извещателя путем помещения его в металлический вкладыш.

б) Создание направленного магнитного поля. Достаточно технологически сложный способ, но воздействие внешнего магнитного поля может ввести извещатель в состояние, когда при размыкании составных частей сигнала проникновения не будет. Внешнее магнитное поле должно быть достаточно мощным.

Этот способ фантастичен, но гипотетически экранирование и использование нескольких извещателей может усложнить и свести к невозможности осуществления такого обхода.

**2.3 Ударно-контактные извещатели**

Обрезка полотна. Данный метод ориентирован на стекло или металл. Используются стеклорез, горелка и т. п. Возможно, предварительно понадобиться демпфирование, например, с помощью резиновых прокладок плотно прижатых к полотну.

Для снижения риска можно использовать более утолщенные полотна и тугоплавкие материалы, использовать дополнительные конструкции (рольставни и т. п.).

**2.4 Пьезоэлектрические извещатели**

Подмена объекта. Этот способ возможен для предметов в музеях, выставках и т. п. Смысл состоит в постепенном подвешивании/установке груза заменителя объекта и снятие охраняемого предмета. Возможно, понадобиться некоторая конструкция, так как вручную это проделать будет почти невозможно.

**2.5 Акустические извещатели**

а) Вырез в полотне. Особенность такого типа извещателей состоит в том, что они реагируют на звуковые волны определенной конфигурации, обычно это звук разбития стекла. Если звуковых волн не будет, то извещатель не сработает. При этом возможен простой выем полотна из рамы, термическое разрушение с помощью горелок, вырезка стеклорезом и т. п.

б) Маскирование. Способ заключается в том, чтобы закрыть датчик звукоотражающим материалом. Для недопущения такого обхода необходимо использовать извещатели с функцией антимаскирования.

**2.6 Ультразвуковые извещатели**

а) Медленная скорость передвижения.

б) Маскирование. Аналогично как в 2.5 б.

в) Использование поглощающих материалов. Злоумышленник окутывается в материал и проходит зону контроля. Для примера, материалом может служить мех, ворсистый ковер и т. п.

**2.7 Активные оптико-электронные извещатели**

а) Засветка приемника. Используется лазер или инфракрасный прожектор. При этом извещатель, конечно же, может сработать, но это зависит от модели. Вспышки и неестественный инфракрасный фон может привести к срабатыванию извещателя, но это зависит от модели. Также, возможно, необходимо расположить приемник так, чтобы было невозможно произвести засветку с неконтролируемой территории.

б) Использование экранов. Под экраном понимается материал препятствующий прохождению волн инфракрасного диапазона. Например, можно взять стеклянное полотно и нести перед собой, при этом все части тела должны быть закрыты стеклом. Предотвратить такой обход можно через использование нескольких извещателей, перекрывающих одну и ту же территорию.

в) Движение рывками или медленное перемещение. Успех данного способа зависит от модели извещателя.

г) Смещение приемника или излучателя. Для двухпозиционных извещателей возможно смещение приемника и излучателя или смещение приемника с применением элемента заменяющего излучатель.

**2.8 Пассивные оптико-электронные извещатели**

а) Маскирование. Самый простой способ - это закраска извещателя полностью или частично с целью изменения зоны обнаружения. При этом, конечно же, нужен доступ злоумышленника к извещателю в то время, когда он не активен.

Предотвращение такого обхода заключается в использовании извещателей с функцией антимаскирования или с контролем саботажной зоны.

б) Засветка или изменение фона. Выполняется через постепенный нагрев необходимой площади до температуры, близкой к температуре тела человека. Другие методы аналогичны 2.7 а. Для защиты необходимо использовать извещатели с функцией защиты от засветки.

в) Использование маскировочных теплоизоляционных плащей и экранов. Такие плащи способны скрыть предмет или человека в инфракрасном диапазоне. Остальное описание данного способа такое же, как и в 2.7 б.

**2.9 Радиоволновые извещатели**

а) Подавление. Воздействие электромагнитным излучением с частотами близкими к рабочим. Защититься от подобного способа обхода можно используя более современные извещатели с функцией обнаружения подобного воздействия.

б) Имитация сигнала или подмена извещателя. При этом используется сторонний радиосигнал, заменяющий основной, а последний в свою очередь удаляется. Защититься от подобного способа обхода можно используя извещатели с функцией защиты собственных сигналов от стороннего анализа.

в) Движения в направлении, перпендикулярном радиальному. Защита: совмещение с другим извещателем, расположенным перпендикулярно радиальному направлению.

г) Движение ползком, перекатами и т. п. Некоторые модели не могут идентифицировать вас как человека и, соответственно, не срабатывают.

д) Экранирования излучения радиоотражающими или радиопоглощающими материалами. Через этот способ можно повлиять на зону обнаружения извещателя. В современных моделях присутствует функция защиты от подобного способа обхода.

**2.10 Все вышеперечисленные а также остальные типы извещателей**

а) Обрезка линии питания/информационного канала. Защита выполняется через маскировку линий, использование различных кожухов, контроль доступа в помещения и к распределительным щиткам, через программный/аппаратный контроль.

б) Отключение от питания. Необходима защита щитков и линий сети питания путем ограничения доступа, а также через маскировку, использование защитных кожухов, через программный/аппаратный контроль. Необходимо обеспечить резервное питание.

**3 Приемо-контрольные приборы**

а) Короткое замыкание участка шлейфа, кратковременные импульсы высокого напряжения. Защита выполняется через использование ПКП с фильтрами, с контролем состояния шлейфа. Также необходим переход с радиальных систем на адресные.

б) Обрыв линии (системы с симплекс режимом). Необходимо переходить к использованию систем с дуплекс режимом.

в) Перехват пакетов, анализ и отсылка ложных сообщений (Ethernet/Internet). Использование систем с достаточной криптографической защитой.

г) Использование технологий подавления и взлома (ПКП использующие телефонные линии). Необходим физический контроль над линией. Также следует использовать более современные и устойчивые системы охраны, отказываясь от устаревших (не меняя канал передачи извещений). Крайний вариант - отказ от такого типа ПКП.

д) Экранирование, зашумление канала (ПКП радиоканальные). Рекомендовано использовать переключающиеся ПКП, использующие несколько каналов передачи извещений.

е) Подавление системами подвижной радиосвязи (ПКП радиоканальные). Решение - переключающиеся ПКП.

ж) Использование моментов перегрузки сети (системы стандарта GSM). Решение - переключающиеся ПКП. При достаточно высоком времени ожидания производится переключение на другой канал передачи.

Литература:


1. http://www.tinko.ru/pdf/7-8-04.pdf
2. http://secandsafe.ru/stati/vzlom_i_proniknovenie/kak_oboyti_ohrannye_izveschateli
3. http://www.tinko.ru/pdf/5-6-02.pdf
4. http://www.teko.biz/support/dokumentacija/normativy/ETT_TCO_.pdf
5. http://www.nicohrana.ru/forum/viewtopic.php?f=18&t=31
6. http://www.nicohrana.ru/forum/viewtopic.php?f=18&t=28
7. http://www.optex.ru/index.php?option=com_content&view=article&id=166&Itemid=334
8. http://vrtp.ru/index.php?act=categories&CODE=article&article=1635
9. http://rutube.ru/video/6ca992a0f1a9289a4ef8c64f0fd19780/
10. http://elementy.ru/news/431286
11. http://www.secuteck.ru/articles2/OPS/perspect_improv_ops_2004/
12. http://www.avanttech.ru/articles/9/94/
13. http://www.kriadon.ru/sistema-kontrolya-i-upravleniya-dostupa.php