И.В. Калиберда

Описание уязвимости внешнего магнитного поля в магнитоконтактных извещателях с описанием способа нейтрализации угрозы саботажа

Для обеспечения целостности информации на объектах информатизации необходимо строгое выполнение требований нормативной документации [3-5]: осуществление физической охраны средств вычислительной техники, предусматривающее постоянное наличие охраны территории и здания, где размещается автоматизированная система, с помощью технических средств охраны. Документ [6] устанавливает требования по оснащению оборудованием периметра здания техническими средствами обнаружения проникновения и угроз различных видов. Дверные конструкции в этом случае контролируют «на открывание» при помощи точечных магнитоконтактных извещателей.

Однако точечные магнитоконтактные извещатели обладают существенной уязвимостью, приводящей к блокированию их основной функции контроля. Зная принцип обнаружения извещателя, основанный на действии магнитного поля, злоумышленники могут использовать действие внешнего магнитного поля (ВМП) для нарушения работоспособности магнитоконтактных извещателей. Приведём описание влияния ВМП на магнитоконтактный извещатель-СМК, установленного на деревянную дверь. Обозначим магнит, входящий в состав извещателя:

магнит №1. В качестве ВМП будем использовать мощный постоянный магнит (магнит №2). Итак, по шагам:

1. Предварительно исследуем полярности магнита №1 в составе охранного извещателя (рисунок 1) и магнита №2, с помощью которого будет осуществляться саботаж. Для этого необходимо воспользоваться компасом.

Рис. 1. Определение полярности магнита №1

При поднесении его к магниту определить, к какому его полюсу притянется северный конец стрелки – это и будет южный полюс нашего магнита. Определение полярности необходимо для того, чтобы при поднесении магнита №2 не поменялась полярность магнита №1 и магнитное поле не было погашено более сильным магнитом, иначе геркон откроется и выдаст тревожное сообщение в шлейф сигнализации, тем самым будет обнаружено действие злоумышленника.

2. Поднести магнит №2 к месту установки охранного извещателя, соблюдая полярность магнита №1, как показано на рисунке 2.

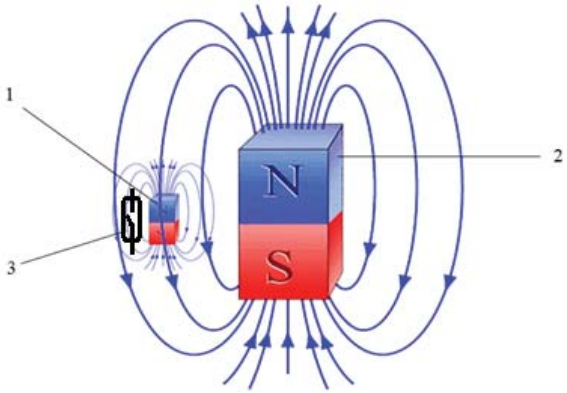

Рис. 2. Схематичное расположение магнитов и геркона относительно друг друга

На рисунке 2 обозначены: 1 – магнит №1 в составе магнитоконтактоного извещателя; 2 – мощный магнит №2 для осуществления саботажа; 3 – геркон, входящий в состав магнитоконтактного извещателя.

3. После того, как мы поднесли магнит №2 с правильной полярностью, дверь можно свободно открыть, не опасаясь того, что сработает охранная сигнализация.

Чтобы защитить магнитоконтактные извещатели от попытки саботажа работы, путем воздействия внешним магнитным полем следует применять датчик внешнего магнитного поля (ДВМП). ДВМП реализуется как блок на основе геркона с переключающимися контактами. ДВМП необходимо установить на одной поверхности с герконом извещателя, как показано на рисунке 3.

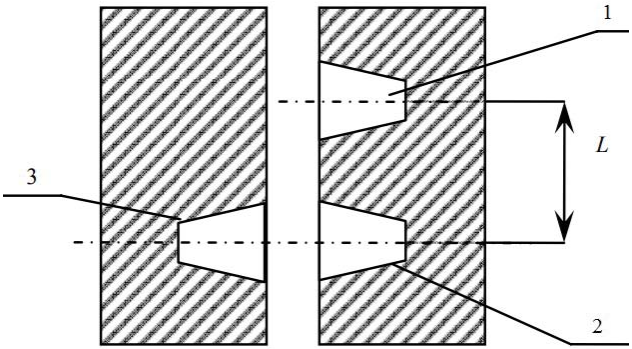

Рис. 3. Схема размещения извещателя и ДВМП

На рисунке 3 обозначены: 1 – ДВМП, 2 – геркон, 3 – магнит в составе извещателя. Расстояние (L) определяется из выражения:

$$L = L_{доп} + L_{изм}, \qquad (1)$$

где:

$L_{доп}$ – максимально допустимое смещение магнита №1 относительно его геркона, указанное в паспорте на извещатель;

$L_{изм}$ – минимальное расстояние смещения магнита №1 относительно ДВМП, при котором нет замыкания контактов ДВМП рядом с магнитом №1.

Наиболее удачным вариантом размещения ДВМП относительно блока извещателя является решение, реализованное в извещателе охранном точечном магнитоконтактном ИО 102-55 «Кенар» (далее Кенар). Кенар конструктивно состоит из двух блоков: исполнительного (магнитоуправляемого датчика) и задающего (управляющего магнита), заключенных в пластмассовые корпуса.

Схема соединений Кенара и световой индикацией состояния герконов представлена на рисунке 4.

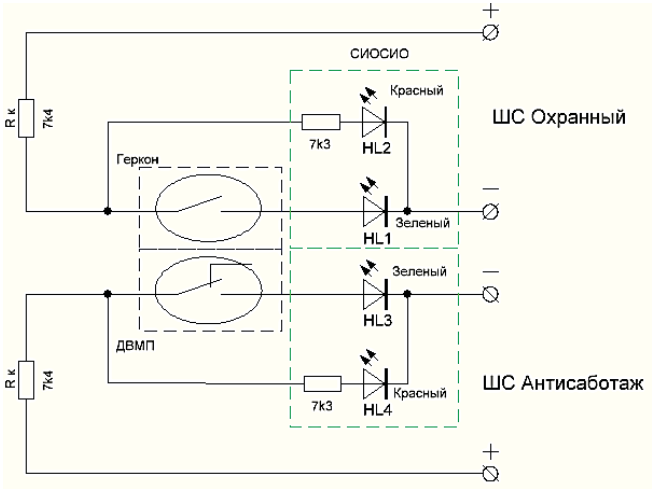

Рис. 4. Схема соединений шлейфов сигнализации совместно с ДВМП и световой индикацией состояния герконов.

В данном случае охранный шлейф сигнализации (ШС) дополняется еще одним ШС, регистрирующим саботаж. Дополнительно применена светодиодная визуализация (СИОСИО) [2], позволяющая контролировать состояния герконов в охранном ШС и ШС «Антисаботаж» (HL1-HL4). Сигнализирующие зелёные светодиоды (HL1, HL3) говорят о том, что охранная сигнализация и ШС «Антисаботаж» находятся в замкнутом состоянии. Это значит, что «дверь закрыта» и внешнее магнитное поле отсутствует. При попытке несанкционированного прохода через дверь происходит размыкание контакта геркона, что приводит к формированию извещения «тревога» («Факт несанкционированного проникновения»): начинает светиться красный светодиод HL2. При попытке саботажа извещателя посредством воздействия магнитом №2 происходит переключение контакта геркона ДВМП, что приводит к блокированию геркона в составе ШС «Охрана», но срабатыванию ШС «Антисаботаж», т.е. формированию извещения «тревога» («Попытка саботажа»): начинает светиться красный светодиод HL4.

В данном описании была рассмотрена уязвимость магнитоконтактного извещателя к действию внешнего магнитного поля и предложена её нейтрализация с помощью датчика магнитного поля. Однако подготовленный нарушитель может вывести из строя и другие типы охранных

извещателей, работа которых основана на разных принципах действий. Акустический извещатель можно саботировать путём перекрытия звукового канала чувствительного элемента, а инфракрасный пассивный извещатель объемного действия – путем маскирования экрана [1: 50], и т.д., в связи с чем в системах инженерно-технической защиты информации предлагается применять охранные извещатели в соответствии с [7] не ниже 3-го класса, обеспечивающие функцию обнаруживать попытку нарушения нормального функционирования путем внешнего воздействия. А в банк данных угроз безопасности информации предлагается включить описание всех выявленных уязвимостей, связанных с саботажем работы охранных извещателей. Предложенные меры будут способствовать правильному выбору средств для защиты от несанкционированного доступа к объектам информации и, как следствие, повышению эффективности защиты информации на объектах информатизации.

Библиографический список

1. Воробьев Г.А., Макаров А.М., Козлов В.А. Разработка математической модели диаграммы направленности охранного извещателя с объёмной зоной обнаружения методом имитационного моделирования // Международное научное издание «Современные фундаментальные и прикладные исследования» / International scientific periodical «Modern fundamental and applied researches». 2017. №2 (25). Часть 1. С. 47-52.
2. Дробот В.А., Решетников В.Н., Шимохин В.Г., Калиберда И.В. Использование индикации для отображения состояния извещателей охранных магнитно-контактных // Молодая наука-2017. Сборник научных трудов V ежегодной научно-практической конференции «Университетская наука – региону»; под ред. Т.А. Шебзуховой, А.А. Вартумяна, И.М. Першина. 2017. С. 61-64.
3. Козлов В.А., Авдусина А.И., Воробьев Г.А., Рындюк В.А. Двухфакторные схемы аутентификации и защиты информации в автоматизированной банковской системе // Университетские чтения – 2017. Материалы научно-методических чтений. Пятигорск, 2017. С. 147-152.
4. Козлов В.А., Рындюк В.А., Воробьев Г.А., Чернышев А.Б. Модели и методы защиты от атак «Man in the middle» (MITM) // Международное научное издание «Современные фундаментальные и прикладные исследования». 2017. № 1 (24). С. 27-35.
5. Методический документ. Утвержден ФСТЭК России 11 февраля 2014 г. Официальный сайт ФСТЭК России. 2014. Дата обновления: 12.01.2015. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument (дата обращения: 18.01.2019).
6. Приказ ФСТЭК России от 11 февраля 2013 г. N 17. Официальный сайт ФСТЭК России. 2013. Дата обновления: 01.12.2014. URL: http:// http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/703-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 18.01.2019).

7. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. Официальный сайт ФСТЭК России. 1992. Дата обновления: 01.12.2014. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g (дата обращения: 18.01.2019).
8. Технические средства обнаружения проникновения и угроз различных видов. Особенности выбора, эксплуатации и применения в зависимости от степени важности и опасности объектов. Рекомендации (Р 78.36.028-2012). М.: НИЦ «Охрана», 2012. 359 с.
9. ГОСТ Р 52435-2015. Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний.
10. Vorobyev G.A., Ryndjuk V.A., Kozlov V.A., Makarov A.M. Probabilistic models of cryptographic systems and their applications // 2016 3rd International Conference on Digital Information Processing, Data Mining, and Wireless Communications, DIPDMWC 2016 3. 2016. С. 160-163.