УДК 004.681.5

АКТИВНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, ПРИМЕНЯЕМЫЕ В АВТОМАТИЗИРОВАННЫХ ПРОИЗВОДСТВАХ

Волхонская Е.Е.[1]
[1]*ФГБОУ ВО «Самарский государственный технический университет», Самара, e-mail: lizaveta5.6@mail.ru*
Чупринина А.С.[1]
[1]*ФГБОУ ВО «Самарский государственный технический университет», Самара, e-mail: anna.chuprinina.02@mail.ru*
Падучих Д.В.[1]
[1]*ФГБОУ ВО «Самарский государственный технический университет», Самара, e-mail: dasha-oleinikova2002@mail.ru*

При разработке технологических процессов и настройки систем их автоматизации требуется учитывать большое количество параметров. Автоматизированные системы состоят из большого количества взаимосвязанных подсистем, каждая из которых выполняют собственную функцию. Функции автоматизированных систем предусматривают большой спектр возможностей, каждая из которых реализуется специфическими программными и техническими комплексами, специализированными на решении определённого рада задач. Автоматизированные системы довольно сложны. Алгоритмы работы, методы и способы для безошибочной работоспособности разрабатывают индивидуально для каждой системы. На производстве необходима защита данной информации. В данной статье будут рассмотрены активные технические средства защиты от утечки по электромагнитному и акустическому каналам, пространственное зашумление, в том числе электромагнитное зашумление и выжигатели телефонных закладных устройств.

Ключевые слова: автоматизированные системы, информация, защита информации

ACTIVE TECHNICAL MEANS OF INFORMATION PROTECTION USED IN AUTOMATED PRODUCTION

Volkhinskaya E.E.[1]
[1]*Samara State Technical University, Samara, e-mail: lizaveta5.6@mail.ru*
Chuprinina A.S.[1]
[1]*Samara State Technical University, Samara, e-mail: anna.chuprinina.02@mail.ru*
Paduchikh D.V.[1]
[1]*Samara State Technical University, Samara, e-mail: dasha-oleinikova2002@mail.ru*

When developing technological processes and configuring their automation systems, it is necessary to take into account a large number of parameters. Automated systems consist of a large number of interconnected subsystems, each of which performs its own function. The functions of automated systems provide a wide range of capabilities, each of which is implemented by specific software and technical complexes specialized in solving a certain set of tasks. Automated systems are quite complex. Algorithms of operation, methods and methods for error-free performance are developed individually for each system. Protection of this information is necessary in the workplace. This article will consider active technical means of protection against leakage through electromagnetic and acoustic channels, spatial noise, including electromagnetic noise and incinerators of telephone embedded devices.

Keywords: automated systems, information, information protection

Активные технические средства защиты

Активное техническое средство защиты – устройство, обеспечивающее создание маскирующих активных помех (или имитирующих их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации.

Активные способы предупреждения утечки информации можно подразделить на обнаружение и нейтрализацию этих устройств[1].

К средствам активной защиты (САЗ) относятся:

1. средства пространственного зашумления;
2. средства экранирования помещений;
3. средства сетевой безопасности.

Активные методы защиты информации направлены на:

1. создание маскирующих пространственных электромагнитных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала ТСПИ;
2. создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях ВТСС с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала ТСПИ.
3. ослабление побочных электромагнитных излучений ТСПИ и их наводок в посторонних проводниках осуществляется путем экранирования и заземления ТСПИ и их соединительных линий.
4. исключение (ослабление) просачивания информационных сигналов ТСПИ в цепи электропитания достигается путем фильтрации информационных сигналов;
5. обнаружение блокировка угроз в режиме реального времени.

Средства активной защиты от утечки по электромагнитному и акустическому каналам

На сегодняшний день виброакустическая защита помещений от прослушивания представляет собой одну из наиболее динамично развивающихся областей защиты информации. В первую очередь это обусловлено уникальными особенностями речевой информации, циркулирующей в помещениях: большим объемом и оперативностью обмена, высокой конфиденциальностью некоторых сообщений, возможностью идентификации личности человека, делающего сообщение, и даже возможностью определения личного отношения говорящего к озвучиваемой информации и составления его психологического портрета. Все это делает проблему защиты акустической информации чрезвычайно важной. В настоящее время на рынке спецтехники разработчиками представлено несколько десятков систем активной защиты акустической информации [2].

Пространственное зашумление

В большинстве случаев для активной защиты воздушных каналов используют системы виброзашумления, к выходам которых подключают громкоговорители. Однако применение динамиков создает не только маскирующий эффект, но и помехи нормальной повседневной работе персонала в защищаемом помещении.

Во время работы вибродатчиков возникают паразитные акустические шумы, вносящие дискомфорт и нарушающие нормальные условия труда в защищаемом помещении.

Увеличение мощности помехи создает повышение уровня паразитного акустического шума, что вызывает дискомфорт у работающих в помещении людей. Это приводит к отключению системы в наиболее ответственные моменты, создавая предпосылки к утечке конфиденциальных сведений. [3]

На рисунке 1 представлено изображение средства виброакустического зашумления «Шорох-2».

Рисунок 1 – Средствовиброакустического зашумления «Шорох-2»

Система «Шорох-2» обеспечивает защиту таких элементов строительных конструкций, как:

1. внешние стены и внутренние стены жесткости, выполненные из монолитного железобетона, железобетонных панелей и кирпичной кладки толщиной до 500 мм;
2. плиты перекрытий, в том числе и покрытые слоем отсыпки и стяжки;
3. внутренние перегородки из различных материалов;
4. остекленные оконные проемы;
5. трубы отопления, водоснабжения, электропроводки;
6. короба систем вентиляции;
7. тамбуры.

Электромагнитное зашумление

Технические средства (ТС) электромагнитного зашумления выполняют одну и ту же задачу: обеспечивают защиту ИО или помещения, где находится ИО, от утечки информации за счет ПЭМИН. Эта защита обеспечивается внесением в каналы утечки такого зашумляющего сигнала, на фоне которого выделить полезный информативный сигнал становится невозможным.

Малогабаритные и маломощные ТС электромагнитного зашумления, обеспечивающие защиту небольшого ИО, называют генераторами шума. Более мощные ТС, способные обеспечить защиту целого помещения или группы помещений, называют системами пространственного зашумления. Во многих случаях генераторы шума и системы пространственного зашумления дополнены некоторыми другими функциями помимо зашумления – например, функциями маскировки информативных побочных электромагнитных излучений и периферийного оборудования, а также радиомикрофонов.

Разделение зашумляющих устройств на генераторы шума и системы пространственного зашумления является довольно условным – точной площади зашумлённого помещения, начиная с которой вместо генератора шума следует применять системы пространственного зашумления никто не установил. [4]

Одним из наиболее распространённых переносных генераторов шума является ГНОМ-3. Изображение данного прибора представлено на рисунке 2.

Рисунок 2 – Переносной генератор шума «ГНОМ-3»

Выжигатели телефонных закладных устройств

Подслушивающие устройства, подключённые к телефонной сети, называются телефонными закладными устройствами. Для их устранения используется метод «выжигания». Метод реализуется путем подачи в линию высоковольтных (напряжение более 1500 В) импульсов, мощностью 15-50 ВА, приводящих к электрическому "выжиганию" входных каскадов электронных устройств перехвата информации и блоков их питания, гальванически подключенных к телефонной линии. [5]

Подача высоковольтных импульсов осуществляется при отключении телефонного аппарата от линии. При этом для уничтожения параллельно подключенных устройств подача высоковольтных импульсов осуществляется при разомкнутой, а последовательно подключенных устройств – при "закороченной" (как правило, в телефонной коробке или щите) телефонной линии.Данный метод реализуют приборы, называемые «выжигателями» на рисунке 3 представлено изображение выжигателя «ГИ-1500».

Рисунок 3 – выжигатель «ГИ-1500»

Средства обнаружения и подавления закладных устройств

Наиболее информативным и легко измеряемым параметром телефонной линии является напряжение в ней при положенной и поднятой трубке. Это обусловлено тем, что в состоянии, когда телефонная трубка положена, в линию подается постоянное напряжение в пределах 60–64 В. При поднятии трубки в линию поступает сигнал, преобразуемый в телефонной трубке в длинный гудок, а напряжение в линии уменьшается до 10–12 В. Если к линии будет подключено закладное устройство, то эти параметры изменятся.

На основе измерений перечисленных параметров и их анализа прибор «принимает» решение о наличии несанкционированных подключений, сигнализирует об изменении параметра линии или наличии в ней посторонних сигналов. Есть приборы, которые кроме блока измерения и анализа параметров, имеют в своем составе и блок для постановки активной заградительной помехи. Примером анализатора телефонных линий является прибор SEC-2004, представленный на рисунке 4.

Рисунок 4 – Индикатор состояния телефонных линий SEC-2004

Список литературы:

1. Пассивные и активные методы и способы защиты каналов утечки информации [Электронный ресурс]//studfile// URL:https://studfile.net/preview/5868802/

2. Активные методы защиты информации от утечки по электромагнитному и акустическому каналам [Электронный ресурс]//Helpiks// URL: https://helpiks.org/8-62604.html

3. Обеспечение сетевой безопасности совместно с брокерами сетевых пакетов. Часть вторая. Активные средства безопасности [Электронный ресурс]// Хабр// URL: https://habr.com/ru/company/dsol/blog/551124/

4. Пассивные и активные средства защиты информации[Электронный ресурс]// Техника для спецслужб // URL:http://www.bnti.ru/showart.asp?aid=547&lvl=04.03.

5. Классификация пассивных и активных способов и средств защиты информации, обрабатываемой техническими средствами. [Электронный ресурс]// Техника для спецслужб // URL:https://cyberpedia.su/5x7b23.html