МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КубГУ»)

Кафедра теоретической экономики

Доклад по дисциплине «Информационная безопасность ИС»
по теме «Физические средства защиты информации»

Работу выполнил _____ 30.11.18 _____ А.А. Гончаров
(подпись, дата)

Факультет экономический

Направление 38.04.05 – Бизнес-информатика

Научный руководитель
док. экон. наук, проф._____ 30.11.2018 _____В.А. Сидоров
(подпись, дата)

Краснодар 2018

Одни из основных средств для решения проблемы защиты информации, используемые для создания механизмов защиты принято считать, технические средства.

Технические средства — это, электрические, электромеханические, электронные и др. типа устройства. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны — недостаточная гибкость, относительно большие объём и масса, высокая стоимость. Вся совокупность технических средств делится на физические и аппаратные.

Рассмотрим физические средства.

Физические средства защиты предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем.

Физические средства по степени сложности делятся на:

– простые;

– сложные;

– системы.

Наряду с традиционными механическими системами при доминирующем участии человека разрабатываются и внедряются универсальные автоматизированные электронные системы физической защиты, предназначенные для охраны территорий, охраны помещений, организации пропускного режима, организации наблюдения; системы пожарной сигнализации; системы предотвращения хищения носителей.

Элементную базу таких систем составляют различные датчики, сигналы от которых обрабатываются микропроцессорами, электронные интеллектуальные ключи, устройства определения биометрических характеристик человека и т. д.

Для организации охраны оборудования, входящего в состав автоматизированной информационной системы предприятия, и перемещаемых носителей информации (дискеты, магнитные ленты, распечатки) используются:

– различные замки (механические, с кодовым набором, с управлением от микропроцессора, радиоуправляемые), которые устанавливают на входные двери, ставни, сейфы, шкафы, устройства и блоки системы;

– микровыключатели, фиксирующие открывание или закрывание дверей и окон;

– инерционные датчики, для подключения которых можно использовать осветительную сеть, телефонные провода и проводку телевизионных антенн;

– специальные наклейки из фольги, которые наклеиваются на все документы, приборы, узлы и блоки системы для предотвращения их выноса из помещения. При любой попытке вынести за пределы помещения предмет с наклейкой специальная установка (аналог детектора металлических объектов), размещенная около выхода, подает сигнал тревоги;

– специальные сейфы и металлические шкафы для установки в них отдельных элементов автоматизированной информационной системы (файл-сервер, принтер и т. п.) и перемещаемых носителей информации.

Для нейтрализации утечки информации по электромагнитным каналам используют экранирующие и поглощающие материалы и изделия. При этом:

– экранирование рабочих помещений, где установлены компоненты автоматизированной информационной системы, осуществляется путем покрытия стен, пола и потолка металлизированными обоями, токопроводящей эмалью и штукатуркой, проволочными сетками или фольгой, установкой загородок из токопроводящего кирпича, многослойных стальных, алюминиевых или из специальной пластмассы листов;

– для защиты окон применяют металлизированные шторы и стекла с токопроводящим слоем;

– все отверстия закрывают металлической сеткой, соединяемой с шиной заземления или настенной экранировкой;

– на вентиляционных каналах монтируют предельные магнитные ловушки, препятствующие распространению радиоволн.

Для защиты от наводок на электрические цепи узлов и блоков автоматизированной информационной системы используют:

– экранированный кабель для внутристоечного, внутриблочного, межблочного и наружного монтажа;

– экранированные эластичные соединители (разъемы), сетевые фильтры подавления электромагнитных излучений;

– провода, наконечники, дроссели, конденсаторы и другие помехоподавляющие радио;

– электроизделия на водопроводных, отопительных, газовых и других металлических трубах помещают разделительные диэлектрические вставки, которые осуществляют разрыв электромагнитной цепи.

Для контроля электропитания используются электронные отслеживатели, устройства, которые устанавливаются в местах ввода сети переменного напряжения. Если шнур питания перерезан, оборван или перегорел, кодированное послание включает сигнал тревоги или активирует телевизионную камеру для последующей записи событий.

Применение специальных генераторов шумов для защиты от хищения информации с компьютеров путем съема ее излучений с экранов дисплеев оказывает неблагоприятное воздействие на организм человека, что приводит к быстрому облысению, снижению аппетита, головным болям, тошноте. Именно поэтому они достаточно редко применяются на практике.

Основные недостатки физических средств защиты являются недостаточная гибкость и громоздкость.

Так же выделим достоинства данных средств:

– надежность функционирования;
– независимость от субъективных факторов;
– высокая устойчивость от модификаций.

ИСТОЧНИКИ

1. Баранова Е., Бабаш А. Информационная безопасность и защита информации, 3-е изд., 2016

2. Малюк А.А. Теория защиты информации, 2014

3. Нестеров С. Основы информационной безопасности, 2016