УДК 004.056.53
DOI 10.21685/2587-7704-2018-3-2-9

Open Access | RESEARCH ARTICLE

Защищенная автоматическая телефонная станция

М. С. Дегтев
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

А. П. Иванов
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. С введением в действие нового нормативного документа по защите информации в декабре 2017 г. к техническим средствам, обрабатывающим сведения, составляющие государственную тайну, стали предъявляться особенно жесткие требования. В этом документе были установлены четкие требования к размеру зоны 2. Это привело к тому, что многие технические средства оказались не пригодны для обработки информации ограниченного доступа. В качестве решения данной проблемы была выбрана доработка технических средств пассивными методами. Наиболее доступным в экономическом плане и в вопросе реализации является изготовление экранирующего корпуса и использование экранированных кабелей.

Ключевые слова: информация, безопасность, побочные электромагнитные излучения и наводки (ПЭМИН), средства разведки, экранирование.

Secure telephone exchange

M. S. Degtev
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

A. P. Ivanov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. There are especially stringent requirements for hardware components processing state secret information with the introduction of a new regulatory document on the information protection in December 2017. This document has established clear requirements for the area of Zone 2. This led to the fact that many hardware components were not suitable for processing information of limited access. As a solution to this problem, the improvement of hardware components by passive methods was chosen. Production of the shielded enclosure and use of shielded cables are the most accessible ways in terms of economy and implementation.

Keywords: information, safety, Transient Electromagnetic Pulse Emanation Standard (TEMPEST), intelligence tools, shielding.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, технические каналы утечки информации можно разделить на электромагнитные, электрические и параметрический [1].

Для перехвата информации иностранные разведки используют различные технические средства разведки. Для перехвата информации, обрабатываемой средствами вычислительной техники (СВТ), используются технические средства разведки побочных электромагнитных излучений и наводок [2].

Побочные электромагнитные излучения (ПЭМИ) возникают при следующих режимах обработки информации:

– вывод информации на экран монитора;
– ввод данных с клавиатуры;
– запись на накопители и чтение информации на накопителе;

– передача данных в каналы связи;

– вывод данных на периферийные печатные устройства и т.д. [2].

Регистрация ПЭМИН может вестись с использованием аппаратуры следующих видов:

– стационарной аппаратуры, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;

– портативной возимой аппаратуры, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;

– портативной носимой аппаратуры;

– автономной автоматической аппаратуры, скрытно устанавливаемой физическими лицами в непосредственной близости от ТСПИ [3].

Типовой комплекс разведки ПЭМИ включает:

– специальное приемное устройство;

– ПЭВМ;

– специальное программное обеспечение;

– широкодиапазонную направленную антенну [2].

Зная характеристики приемного устройства и антенной системы средства разведки, можно рассчитать допустимое (нормированное) значение напряженности электромагнитного поля, при котором вероятность обнаружения сигнала приемным устройством средства разведки будет равна некоторому (нормированному) значению [2].

Опасной зоной 2 называется пространство вокруг ТСПИ, на границе и за пределами которого напряженность электрической или магнитной составляющей электромагнитного поля не превышает допустимого (нормированного) значения [2].

Размер зоны 2 для каждого СВТ определяется инструментально-расчетным методом при проведении специальных исследований СВТ на ПЭМИ и указывается в предписании на их эксплуатацию или сертификате соответствия [2].

Защищенная автоматическая телефонная станция – техническое средство, реализующее коммутационные функции и соответствующее требованиям нормативных документов по защите информации. В состав станции входит IP-АТС «Агат РТ UX-3410».

В ходе проведения лабораторных специальных исследований измерялись побочные электромагнитные излучения от мини IP-АТС «АГАТ-РТ UX-3410». IP-АТСАГАТ входит в состав комплекта оборудования специальной связи (КОСС).

Полученные в ходе специальных исследований радиусы контролируемых зон (КЗ) в зависимости от категории объекта и типа средств разведок приведены в табл. 1.

Таблица 1

Радиусы контролируемых зон

	Размеры зон R2, м			r1,м	r1′,м
	Стационарные средства разведки	Портативные возимые средства разведки	Портативные носимые средства разведки		
Категория 1	1000	480	205	25	3
Категория 2	405	140	60	7	2
Категория 3	240	80	35	6	2

Примечание. R2 – величина максимально возможной зоны разведки побочных электромагнитных излучений; r1 – требуемое расстояние от технического средства до сосредоточенных случайных антенн (телефонные аппараты, элементы связной и измерительной аппаратуры и т.п.), имеющих выход за пределы КЗ; r1′ – требуемое расстояние от технического средства до распределенных случайных антенн (посторонние провода и кабели вспомогательных технических средств, линии связи, коммуникации и т.п.), выходящих за пределы контролируемой зоны.

Из табл. 1 видно, что требования руководящего документа по защите информации, содержащей сведения, составляющие государственную тайну, не выполняются для возимых средств разведки. Следовательно, обработка информации, содержащей сведения, составляющие государственную тайну, с использованием IP-АТС UX-3410 запрещена. В связи с этим IP-АТС должна быть доработана пассивными методами для соответствия требованиям нормативных документов по защите информации.

Защита информации от утечки через ПЭМИН может осуществляться с использованием пассивных или активных методов и средств.

Пассивные методы защиты информации направлены на:

– ослабление побочных электромагнитных излучений основных технических средств и систем (ОТСС) на границе контролируемой зоны;

– ослабление наводок побочных электромагнитных излучений в посторонних проводниках и соединительных линиях, выходящих за пределы контролируемой зоны;

– исключение или ослабление просачивания информационных сигналов в цепи электропитания, выходящие за пределы контролируемой зоны [3].

Активные методы защиты информации направлены на:

– создание маскирующих пространственных электромагнитных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны;

– создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях с целью уменьшения отношения сигнал/шум на границе контролируемой зоны [3].

Одним из наиболее эффективных пассивных методов защиты от ПЭМИ является экранирование. Экранирование – это локализация электромагнитной энергии в определенном пространстве за счет ограничения распространения ее всеми возможными способами [3].

Существует три вида экранирования:

– электромагнитное;

– электростатическое;

– магнитостатическое [3].

Электростатическое и магнитостатическое экранирование основано на замыкании экраном (обладающим в первом случае высокой электропроводностью, а во втором магнитопроводностью), соответственно, электрического и магнитного полей [4].

Электростатическое экранирование сводится к замыканию электростатического поля на поверхность металлического экрана и отводу электрических зарядов на землю (на корпус прибора). Заземление электростатического экрана является необходимым элементом при реализации электростатического экранирования [4].

Для выбора материала экрана необходимо учитывать требуемую эффективность экранирования в заданном диапазоне частот при определенных ограничениях. Такие ограничения обычно связаны с массогабаритными характеристиками экрана, влиянием экрана на экранируемый объект, с прочностью и устойчивостью экрана против коррозии, с технологичностью его конструкции и другими факторами [3].

Для изготовления экранов могут использоваться:

– металлические материалы;

– материалы-диэлектрики;

– стекла с токопроводящим покрытием;

– специальные металлизированные ткани;

– токопроводящие краски [3].

Наряду с техническими средствами экранированию также подлежат монтажные провода и соединительные линии. Экранированные провода и кабели следует применять в основном для соединения отдельных блоков и узлов друг с другом [3].

Библиографический список

1. Хорев, А. А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации / А. А. Хорев. – URL: http://www.analitika.info/kanalutechki.php (дата обращения: 01.10.2018).
2. Хорев, А. А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники / А. А. Хорев. – URL: http://www.bnti.ru/showart.asp?aid=954&lvl=04.03. (дата обращения: 01.10.2018).
3. Информационный ресурс: Интуит. Лекция 16: Методы защиты информации от утечки через ПЭМИН. – URL: http://www.intuit.ru/studies/courses/2291/591/lecture/12704 (дата обращения: 01.10.2018).
4. Хорев, А. А. Способы защиты объектов информатизации от утечки информации по техническим каналам: экранирование / А. А. Хорев. – URL: http://www.bnti.ru/showart.asp?aid=985&lvl=04. (дата обращения: 01.10.2018).

Дегтев, М. С.

Защищенная автоматическая телефонная станция / М. С. Дегтев, А. П. Иванов // Инжиниринг и технологии. – 2018. – Vol. 3(2). – DOI 10.21685/2587-7704-2018-3-2-9.