Защита от электронного шпионажа

В.П. Иванов

В последние годы большое внимание уделяется защите информации, обрабатываемой с помощью вычислительной техники. Утечка информации может произойти как при несанкционированном доступе к базам данных, так и при перехвате побочных электромагнитных излучений (ПЭМИ). Чувствительная радиоэлектронная аппаратура позволяет уловить ПЭМИ и полностью восстановить обрабатываемую компьютером информацию. Диапазон излучаемых колебаний простирается от десятков килогерц до 1000 МГц и определяется частотой задающего генератора ПК. Для мониторов максимум информационных излучений обычно находится в диапазоне 100 — 350 МГц. Следует иметь в виду, что для восстановления информации пригодна любая гармоника (вплоть до 30-й) тактовой частоты.

Устройства вычислительной техники помимо высокочастотных создают и низкочастотные магнитные и электрические поля, интенсивность которых быстро убывает с расстоянием. Тем не менее они способны вызвать значительные по величине наводки в близко расположенных проводных цепях, например в охранной сигнализации, телефонных линиях, силовой сети, металлических трубах и т. д. Напряженность этих полей существенна на частотах от десятков килогерц до десятков мегагерц. Чтобы перехватить информацию, которую несут в себе низкочастотные колебания, приемную аппаратуру подключают непосредственно к коммуникациям за пределами охраняемой территории.

Криптографическую защиту применяют при обмене информацией между компьютерами по линиям передачи или в случае обработки данных, но не используют при выводе информации на периферийные устройства, такие, как монитор, принтер и накопитель информации. Поэтому наиболее опасными компонентами вычислительных систем с точки зрения утечки информации через побочные излучения являются мониторы ПК. Следует отметить, что в Россию запрещен импорт защищенных от электронного шпионажа компьютеров и сетевого оборудования. Поэтому ниже мы приводим описание устройств маскировки информации отечественного производства.

Способы защиты и маскировки информации

Наряду с организационными, программными, криптографическими способами защиты информации от перехвата применяют:

- доработку устройств вычислительной техники для минимизации излучений;

- электромагнитное экранирование устройств и помещений, где расположены компьютерные системы;

- активную радиотехническую маскировку.

Доработка устройств вычислительной техники позволяет существенно уменьшить уровень информационных излучений, но, к сожалению, устранить их полностью не удается. К тому же стоимость выполнения этих работ, как правило, соизмерима со стоимостью защищаемой вычислительной системы.

Действенным способом защиты информации от перехвата на радиочастотах является электромагнитное экранирование, но оно требует значительных капитальных вложений и регулярного контроля эффективности. Кроме того, полное экранирование может повлиять на здоровье обслуживающего персонала, а реализовать подобную защиту в офисах коммерческих фирм вообще не представляется возможным.

Активная радиотехническая маскировка побочных электромагнитных излучений заключается в формировании вблизи от устройств вычислительной техники широкополосного шумового сигнала с уровнем, превышающим уровень информационных излучений в заданное число раз (как того требуют нормативные документы Гостехкомиссии России) во всем частотном диапазоне. Также, согласно этому методу, необходимо генерировать наводки, маскирующие паразитные колебания в системах коммуникаций.

Техническая реализация устройств маскировки

В специальном конструкторском бюро Института радиотехники и электроники (ИРЭ) РАН разработаны малогабаритные сверхширокополосные передатчики шумовых колебаний

ГШ-1000 и ГШ-К-1000, которые являются модернизацией известного изделия “Шатер-4”. Принцип их работы основан на реализации сложных нелинейных процессов в генераторе. Усиленный шумовой сигнал излучается с помощью активной антенны. Она обеспечивает необходимое распределение по частотному диапазону спектральной плотности маскирующего электромагнитного поля и наводит низкочастотные колебания в отходящие цепи. По статистическим характеристикам колебания близки к белому шуму.

Модель ГШ-1000, предназначенная для маскировки ПК, других компьютерных систем и сетей, выполнена в виде отдельной конструкции с питанием от сети. Ее располагают на расстоянии 1,5 — 5 м от устройств вычислительной техники. Генератор ГШ-К-1000 изготавливается в виде платы, устанавливаемой в гнездо системного блока ПК. Обе модели сертифицированы Гостехкомиссией России.

По сравнению с аналогичными по назначению изделиями “Гном”, “Сфера”, “Смог”, “Октава” рассматриваемые генераторы шума обладают повышенным коэффициентом качества маскирующего сигнала, круговой поляризацией излучения, имеют меньшие вес и размеры, более удобны в эксплуатации.

Генераторы шума обеспечивают надежную маскировку побочных излучений принтеров, плоттеров, устройств ввода-вывода, мониторов и т. д.

в помещении площадью до 50 кв.м. В случае большей площади необходимо устанавливать несколько устройств.

Интенсивность излучаемого маскирующего сигнала не превышает допустимых норм на промышленные радиопомехи, поэтому согласования установки генераторов шума со службой радиоконтроля не требуется. Кроме того, генераторы не влияют на работу вычислительной техники даже при размещении в непосредственной от нее близости.

Генераторы могут быть подключены без труда, однако при их установке необходима консультация специалистов для проверки эффективности защиты.