СНИЖЕНИЕ УРОВНЯ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ВИДЕОТРАКТА ПЕРСОНАЛЬНОЙ ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНОЙ МАШИНЫ С ИСПОЛЬЗОВАНИЕМ ПОДБОРА ЦВЕТА ТЕКСТА И ФОНА

Н.А.Титович, А.И. Майоров, Д.А. Высоцкий

Угроза утечки конфиденциальной информации, обрабатываемой на персональной электронно вычислительной машине (далее – ПЭВМ), по каналу побочных электромагнитных излучений (далее – ПЭМИ) известна достаточно давно. Особая опасность состоит в том, что даже в случае использования криптографических методов защиты на ПЭВМ угроза утечки по каналу ПЭМИ остается актуальной – злоумышленник может перехватить информацию от составных частей ПЭВМ, которые обрабатывают незашифрованную информацию. Видеотракт ПЭВМ, как правило, обладает наибольшим уровнем излучения ПЭМИ. В настоящее время существует два основных способа защиты информации от утечки по рассматриваемому каналу утечки: пассивный (экранирование ПЭВМ либо помещения, в котором размещена ПЭВМ) и активный (применение генераторов электромагнитного шума в непосредственной близости от ПЭВМ). Предлагаемый метод защиты видеотракта ПЭВМ применим для ПЭВМ, использующих интерфейс VGA. Информация в интерфейсе VGA передается в аналоговом виде по трем цветовым каналам и двум каналам синхронизации: строчному и кадровому. ПЭМИ видеотракта с интерфейсом VGA имеет схожую структуру с аналоговым телевизионным сигналом и представляет суперпозицию излучений трех цветовых сигналов и сигналов синхронизации. Цвет каждого пикселя задается уровнем каждого цветового сигнала. Соответственно, чтобы снизить уровень ПЭМИ необходимо выбирать максимально возможные темные цвета фона и текста, отображаемые на мониторе. Также необходимо максимально затруднить возможность различения злоумышленником текста и фона, этого можно достичь таким подбором цвета текста и фона, при котором сумма напряжений трех цветовых сигналов фона будет равна сумме напряжений цветовых каналов текста. Однако, необходимо сохранить удобство работы пользователя ПЭВМ. Человеческий глаз наиболее восприимчив к зеленому цвету. Проведенные исследования показали, что наиболее читаемым оказался зеленый текст на фоне с оттенками зеленого. Цвета удовлетворяют условию, описанному выше. Таким образом, с помощью представленного метода, можно значительно снизить уровень ПЭМИ, что уменьшит зону технической разведдоступности ПЭВМ и максимально усложнит задачу детектирования принятой злоумышленником информации.

Литература

1. Kuhn M.G. Electromagnetic eavesdropping risks of flat-panel displays [Electronic resource]. – URL: https://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf (date of access: 01.05.2018).

2. Филиппович А.Г. Побочные электромагнитные излучения видеотракта ПЭВМ // Управление защитой информации. 2008. Т. 12, № 1. С. 92–97.

МАЛОГАБАРИТНЫЙ ТЕСТОВЫЙ ГЕНЕРАТОР РАДИОПОМЕХ

А.В. Толмачев, В.М. Чертков

Малогабаритный тестовый генератор радиопомех разработан с целью испытаний радиолокационного оборудования в условиях широкого применения условным противником средств РЭБ с использованием различных тактических приемов. Для полноценной имитации тактической обстановки и формирования тактико-технических требований к генератору радиопомех выполнены: анализ характеристик перспективных отечественных радиолокационных станций [1], анализ применения активного элемента генератора, анализа возможных схем построения с выбранным активным элементом, анализ и выбор типа антенной системы [2]. Рассмотренные тактико-технические требования к имитатору помеховой обстановки позволили определить его общую структурную схему. Была выбрана и обоснована элементная база, выработано наиболее оптимальное схемное решение, которое обеспечивает требования по механической прочности, скрытности, транспортабельности, универсальности,

частотному диапазону, мощности и виду создаваемых помех, что позволило применять его в ходе испытаний радиолокационного обнародования и радиолокационных станций. Выполненное имитационное моделирование и проведенные натурные эксперименты позволили оценить эксплуатационную надежность малогабаритного тестового генератора радиопомех. Разработанный генератор радиопомех возможно использовать в качестве забрасываемого передатчика помех, который будет достаточно эффективным средством для усложнения работы радиолокационных средств противника, а также для тренировки работы операторов на радиолокационных станций, стоящих в настоящее время на вооружении.

Литература

1. Радиолокационная станция обнаружения маловысотных наземных объектов X-диапазона «Родник» [Электронный ресурс]. – URL: http://www.kbradar.by/products/radiolokatsiya/radiolokatsionnye-stantsii/519/ (дата обращения: 10.04.2018).

2. Охрименко А.Е. Основы радиолокации и радиоэлектронная борьба. Ч.1. Москва: Воениздат, 1983. 457 с.

КЛЮЧЕВЫЕ АСПЕКТЫ ПРОЦЕССА МОДЕЛИРОВАНИЯ РИСКОВ ДЛЯ ИНФОРМАЦИОННОЙ СЕТИ ОРГАНИЗАЦИИ

А.В. Федорцов

Реализация эффективного управления информационной безопасностью (ИБ) в организации связана, в первую очередь, с формализацией координированных действий по руководству и управлению организацией в отношении рисков для материальных активов из состава информационной инфраструктуры. Менеджмент рисков [1], как правило, заключается (но не ограничивается) в последовательном выполнении следующих шагов: оценка рисков, обработка рисков, принятие рисков, обмен информацией о рисках. К ключевым аспектам процесса моделирования рисков для информационной сети организации следует относить вычисление значений вероятностей возникновения особого набора обстоятельств совершения атак на информационную инфраструктуру и ущерба (последствий) от таких событий ИБ для материальных активов [2], необходимых для выполнения количественной оценки рисков. Ввиду отсутствия универсального подхода к количественной оценке ущерба, позволяющего определить результат воздействия на программно-технические средства из состава информационной сети организации, решить задачу оценки последствий можно рассчитав прямой и косвенный ущерб соответствующим материальным активам. Прямой ущерб предлагается отражать как сумму отношений показателей функционирования программно-технических средств до и после совершения атаки либо отношений дополнительной стоимости затрат на восстановление оптимальных показателей функционирования к уже вложенным денежным средствам. Косвенный ущерб при этом будет характеризоваться суммой произведений определенных для организации весовых коэффициентов основных свойств обрабатываемой в информационной сети информации (конфиденциальность, целостность, сохранность и доступность) и количества атакованных материальных активов, обрабатывающих информацию.

Литература

1. СТБ ISO/IEC 27000-2012. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь.

2. Федорцов А.В., Кучинский П.В. Роль и место оценки ущерба от атак внутренних нарушителей в процессах управления информационной безопасностью организаций // Управление информационными ресурсами : материалы XIII Междунар. науч.-практ. конф. Минск, 9 декабря 2016 г. С. 205.