УДК 621.396

С.В. Рыженко, А.В. Радионов

Россия, г. Королёв, Частное учреждение дополнительного профессионального образования «Учебный центр ЦБИ»

О СПОСОБАХ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ЗА СЧЁТ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И АТТЕСТАЦИИ ОБЪЕКТОВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

В статье предложен подход к решению задачи выбора способа создания системы защиты информации от утечки за счёт побочных электромагнитных излучений и аттестации объектов информатизации для требуемого количества защищаемых средств вычислительной техники на начальном этапе проектирования для установленных экспертным путем технико-экономических условий.

Ключевые слова: средство активной защиты; техническое средство; средство вычислительной техники; генератор шума; объект информатизации.

В настоящее время для защиты объектов вычислительной техники (ОВТ) от утечки за счёт побочных электромагнитных излучений (ПЭМИ) 177ннованиются средства активной защиты (САЗ), представляющие собой отдельные генераторы электромагнитного шума (ГШ) или их совокупности (системы) [1]. Наиболее распространенными методами, применяемыми для активной защиты информации от утечки за счёт ПЭМИ, являются методы совмещённого и распределённого размещения ГШ [2].

При совмещённом использовании генераторы шума устанавливаются в непосредственной близости относительно средств вычислительной техники, предназначенных для обработки защищаемой информации (ЗСВТ), порой такие генераторы шума называют маскираторами [3].

Распределённый метод защиты допускает установку автономных ГШ, пространственно-разнесённых относительно ЗСВТ, групповое размещение ГШ или применение системы защиты, состоящей из нескольких САЗ [4].

Выбор способа создания системы защиты информации от утечки за счёт побочных электромагнитных излучений и аттестации объектов информатизации осуществляется из трех применяемых на сегодняшний день подходов [5]:

– автономный (генератор шума используется в составе объекта вычислительной техники, включающего одно ЗСВТ);

– групповой (генераторы шума используются для защиты нескольких объектов вычислительной техники, имеющих в своём составе по одному ЗСВТ);

– системный (генераторы шума объединены в пространственную систему и используются для защиты нескольких ЗСВТ, входящих в состав единого объекта вычислительной техники).

Для каждого из трех подходов представляется возможным оценивать совокупность трудозатрат по защите объектов информатизации на базе средств вычислительной техники и их аттестации: $\mathrm{С}_{\text{авт,}}$ – при автономном подходе, $\mathrm{С}_{\text{гр}}$ – групповом, $\mathrm{С}_{\text{сист}}$ – системном.

Полученные оценки сопоставляются друг с другом путём расчёта разницы трудозатрат для рассматриваемых подходов:

$$\begin{cases} \Delta\mathrm{С}_{I} = \mathrm{С}_{\text{авт}} - \mathrm{С}_{\text{гр}}, \\ \Delta\mathrm{С}_{II} = \mathrm{С}_{\text{авт}} - \mathrm{С}_{\text{сист}}, \\ \Delta\mathrm{С}_{III} = \mathrm{С}_{\text{гр}} - \mathrm{С}_{\text{сист}}; \end{cases}$$

Выбор экономически выгодного подхода предлагается осуществлять по критерию:

$$\begin{cases} \text{АВТОНОМНЫЙ, если } (\Delta\mathrm{С}_{I} \le \Delta S) \cap (\Delta\mathrm{С}_{II} \le \Delta S), \\ \text{ГРУППОВОЙ, если } (\Delta\mathrm{С}_{I} > \Delta S) \cap (\Delta\mathrm{С}_{III} \le \Delta S), \\ \text{СИСТЕМНЫЙ, если } (\Delta\mathrm{С}_{II} > \Delta S) \cap (\Delta\mathrm{С}_{III} > \Delta S), \end{cases}$$

где $\Delta S = (\max\limits_{k \,\epsilon\, K} S_k - \min_{k \,\epsilon\, K} S_k)$ – значение максимального превышения оценки трудозатрат при выборе организации-исполнителя специальных работ из опрошенного множества организаций K с трудозатратами S_k, включающих аттестацию объекта информатизации, состоящего из одного ЗСВТ и защищаемого одним САЗ:

$$S_k = {}_k\mathrm{С}_{\text{авт}_1} = {}_k\mathrm{С}_{\text{гр}_1} = {}_k\mathrm{С}_{\text{сист}_1}, k \,\epsilon\, K,$$

где ${}_k\mathrm{С}_{\text{авт}_1}, {}_k\mathrm{С}_{\text{гр}_1}, {}_k\mathrm{С}_{\text{сист}_1}$ – стоимость проведения защитных мероприятий и аттестации объекта информатизации, состоящего из одного ЗСВТ, с применением единственного генератора шума.

Совокупность трудозатрат для различных подходов предлагается определить из технико-экономических показателей, выраженных в трудозатратах, перечень которых приведён в таблице 1.

Таблица 1 – Технико-экономические показатели защиты и аттестации ОВТ

п/п	Наименование показателя	Условное обозначение
2.	Обследование объекта информатизации	C_1
3.	Разработка программы аттестационных испытаний объекта информатизации	C_2
4.	Проведение специальной проверки технических средств	C_3
5.	Проведение специальных исследований технических средств	C_4
6.	Контроль защищённости обрабатываемой информации	C_5
7.	Разработка системы защиты информации	C_6
8.	Закупка, поставка средств активной защиты информации	C_7
9.	Монтаж и настройка средств активной защиты	C_8
10.	Разработка инструкции по эксплуатации средств активной защиты	C_9
11.	Закупка, поставка средств защиты от несанкционированного доступа	C_{10}
12.	Закупка, поставка антивирусной программы	C_{11}
13.	Установка и настройка средств защиты от несанкционированного доступа	C_{12}
14.	Установка и настройка антивирусной программы	C_{13}
15.	Оценка эффективности средств активной защиты информации	C_{14}
16.	Проведение комплексных аттестационных испытаний объекта информатизации	C_{15}
	Сумма	S

Для автономной системы защиты информации трудозатраты составляют количество защищаемых СВТ, умноженное на трудозатраты на выполнение защитных мероприятий и аттестации одного объекта информатизации. Совокупность трудозатрат, включая закупку и поставку средств защиты, рассчитывается по формуле [6]:

$$\mathrm{C}_{\text{авт}} = N_{\text{ЗСВТ}} \cdot \sum_{n=1}^{15} C_n,$$

где $N_{\text{ЗСВТ}}$ – количество защищаемых СВТ.

Если использовать средства активной защиты информации от утечки за счёт побочных электромагнитных излучений для группы ЗСВТ, то трудозатраты складываются из работ по разработке единой системы защиты информации от утечки за счёт побочных электромагнитных излучений, работ по закупке и монтажу средств активной защиты для всех СВТ и работ по подготовке и аттестации каждого ОВТ.

Совокупность трудозатрат рассчитывается по формуле:

$$\mathrm{C}_{\text{гр}} = \mathrm{C}_{\text{саз}} + N_{\text{гш}} \cdot \sum_{n=7}^{8} C_n + N_{\text{ЗСВТ}} \cdot \sum_{n=1-5;\,9-15} C_n,$$

где: $N_{\text{гш}}$ – количество генераторов шума (средств активной защиты),

$\mathrm{C}_{\text{саз}}$ – трудозатраты на разработку системы защиты.

В качестве допущения примем, что затраты $\mathrm{C}_{\text{саз}}$ для группового и автономного подходов превышают не менее чем в K_p раз затраты C_6:

$$\mathrm{C}_{\text{саз}} = K_p \mathrm{C}_6$$

Для системного подхода трудозатраты складываются из затрат на разработку единой системы защиты, работ по закупке и монтажу средств активной защиты, работ по подготовке основных технических средств к аттестации и работ по аттестации единого объекта вычислительной техники. Совокупность трудозатрат рассчитывается по формуле:

$$\mathrm{C}_{\text{сист}} = C_{\text{саз}} + N_{\text{гш}} \cdot \sum_{n=7}^{8} C_n + N_{\text{ЗСВТ}} \cdot \sum_{n=1;3-5;\,10-14} C_n + \sum_{n=2;9;15} C_n$$

Таким образом, при построении системы защиты информации от утечки за счёт побочных электромагнитных излучений применительно к принятым технико-экономическим условиям возможно определить целесообразность использования способа создания системы защиты информации от утечки за счёт побочных электромагнитных излучений и аттестации объектов информатизации для требуемого количества защищаемых СВТ.

Предложенный методический подход позволяет определить указанную целесообразность на начальном этапе проектирования для установленных экспертным путем технико-экономических условий.

Литература

1. Парфенов В.И. Защита информации. Словарь. Воронеж, 2003.

2. Сборник методических документов ФСТЭК России, 2005.

3. Хорев А.А. Оценка возможности по перехвату побочных электромагнитных излучений видеосистемы компьютера. Часть 2 // Специальная техника. – № 4. – 2011.

4. Рыженко С.В., Василенко В.В. Увеличение жизненного цикла защищённых объектов вычислительной техники за счёт построения пространственной системы активной защиты информации распределённого объекта информатизации, обеспечивающей защищённость по каналу побочных электромагнитных излучений от основных технических средств и систем // Научно-практический журнал. Материалы XIV Международной научно-практической конференции «Информационная безопасность – 2015». – Таганрог, 2015.

5. Кондратьев А.В. Техническая защита информации. Практика работ по оценке основных каналов утечки – Москва, 2016.

6. Выгодский М.Я. Справочник по высшей математике. – М: Наука, 1966.