С.В. Скрыль,
доктор технических наук, профессор;
С.С. Никулин,
кандидат технических наук, доцент;
В.О. Крылов

МЕТОДИКА ОЦЕНКИ ОБЪЕМА ИНФОРМАЦИИ, РАСКРЫВАЕМОЙ В ПРОЦЕССЕ ПЕРЕХВАТА ИНФОРМАТИВНЫХ СИГНАЛОВ ОТ ОСНОВНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ И СИСТЕМ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

TECHNIQUE OF ASSESSMENT OF VOLUME OF INFORMATION OPENED IN THE COURSE OF INTERCEPTION OF INFORMATIVE SIGNALS FROM THE FIXED TECHNICAL MEANS AND SYSTEMS ON OBJECTS OF INFORMATIZATION

В статье приведена методика оценки объема информации, раскрываемой в процессе перехвата информативных сигналов побочных электромагнитных излучений и наводок от основных технических средств и систем на объектах информатизации. Показано, что данная методика является предпосылкой для синтеза адекватной модели распознавания подобного рода угроз информационной безопасности.

The technique of assessment of volume of information opened in the course of interception of informative signals of collateral electromagnetic radiations and aimings from the fixed technical means and systems on objects of informatization is given in article. It is shown that this technique is a prerequisite for synthesis of adequate model of recognition of this sort of threats of information security.

Теория распознавания, в своих приложениях в области технической защиты информации [1], при распознавании угроз утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН) [2] от основных технических средств и систем (ОТСС) [3] объектов информатизации (ОИ) предполагает оценку следующих параметров:

1) этапа реализации угрозы;
2) объема информации, раскрываемой в процессе перехвата;
3) возможности по реагированию на такого рода угрозу.

При этом как с методической, так и с практической точек зрения задача оценки объема информации, раскрываемой в процессе перехвата, является наиболее сложной.

С целью разработки методики решения данной задачи воспользуемся рядом приведенных в [4] теоретических положений, основанных на установленных аналитических соотношениях между функциональными характеристиками процессов обработки и обмена информацией и процессов ее перехвата техническими средствами разведки (ТСР). В соответствии с этими положениями значение своевременности реализации процедур обработки и обмена информацией на ОИ определяется как:

$$a = 1 - \frac{\sum_{n=1}^{N} \delta_n}{N}, \qquad (1)$$

где $\delta_n = \begin{cases} 1, \textit{если } \beta \cdot \tau_{(ou)n} \le \tau_{(p)n}; \\ 0, \textit{если } \beta \cdot \tau_{(ou)n} > \tau_{(p)n}, \end{cases}$

$\tau_{(ou)n}$ – время реализации n – й процедуры обработки и обмена информацией;

$\tau_{(p)n}$ – время раскрытия содержания информации при реализации n – й процедуры ее обработки и обмена;

β - коэффициент, определяющий величину перехваченной части сообщения, соответствующую раскрытию его содержания;

N – число выполненных процедур обработки и обмена информацией на временном интервале исследования работы ОТСС на ОИ.

С формальной точки зрения отсутствие утечки информации по каналам ПЭМИН от ОТСС на ОИ соответствует нулевому значению времени $\tau_{(p)n}$. В этом случае показатель своевременности (1) равен единице.

Ситуация наличия канала утечки информации рассматриваемого типа будет интерпретироваться как ситуация, при которой в сообщениях перехватывается не менее заданной их части. Повышение уровня угрозы утечки информации при этом влечет за собой увеличение значения $\tau_{(p)n}$ и, как следствие, уменьшение показателя a от единицы до нуля. Исходя из изложенного, существует критическое значение $\tau_{(ркр)}$ времени раскрытия содержания информации, при котором реализация любой из процедур ее обработки и обмена, вследствие утечки информации, теряет смысл:

$$\tau_{(ркр)} = \beta \cdot \tau_{(ou)}, \qquad (2)$$

где $\tau_{(ou)}$ – время реализации информационных процессов на ОИ на временном интервале $[t_1, t_2]$.

Определим соотношение между объемом $V_{(p)}$ раскрытой информации от ОТСС ОИ, вследствие ее утечки по каналам ПЭМИН, и значениями $\tau_{(ркр)}$ и $\tau_{(ou)}$:

$$\frac{V_{(p)}}{V} = \frac{\tau_{(ркр)}}{\tau_{(ou)}}, \qquad (3)$$

где V – объем информации, обработанной ОТСС ОИ за время t_2 - t_1.

Величину:

$$\alpha = \frac{V_{(p)}}{V} \qquad (4)$$

будем рассматривать в качестве характеристики доли раскрытой информации относительно всего ее объема, обработанного ОТСС ОИ за время t_2 - t_1.

Подставив (2) в (3) выражение (4) можно представить в виде равенства:

$$\alpha = \beta. \qquad (5)$$

На множестве идентифицируемых функций противоправных действий по перехвату информативных сигналов ПЭМИН:

$$\{\varphi_{l1\ l2\ l3}\}, \qquad (6)$$

где $l1$, $l2$, $l3$ – индекс идентифицируемой функции, характеризующий ее структурную взаимосвязь в композиционной структуре модели распознавания подобного рода угроз [1],

определим подмножество:

$$\{\varphi_{k1\ k2\ k3}\} \qquad (7)$$

функций, связанных с формированием множества перехваченных сообщений. Исходя из содержания представленной в [5] функциональной модели процесса перехвата информативных сигналов ПЭМИН, данное множество составят следующие функции:

φ_{511} – преобразование сигналов ПЭМИН в телекоммуникационные данные, данные изображений;

φ_{512} – преобразование телекоммуникационной информации в удобный для анализа вид, подбор контрастности изображений и удаление избыточной информации, перехваченной по каналам ПЭМИН;

φ_{513} – формирование базы данных перехваченной информации;

φ_{521} – формирование поискового запроса для системы управления базами данных (СУБД);

φ_{522} – восстановление исходных параметров перехваченной информации корреляционными методами;

φ_{531} – анализ раскрытой информации, обрабатываемой на ОИ на предмет достаточности её для раскрытия содержания информационного процесса;

φ_{532} – анализ раскрытой информации, обрабатываемой на ОИ на предмет содержания в ней возможной дезинформации.

Представим значение β как отношение времени, затраченного нарушителем на реализацию последовательности функций, связанных с формированием множества (7), к времени формирования этого множества:

$$\beta = \frac{\sum_{j=1}^{J} \tau_j}{\sum_{i=1}^{I} \tau_i} = \frac{\gamma}{\sum_{i=1}^{I} \tau_i}, \qquad (8)$$

где τ_i – время реализации i-ой, i = 1, 2, ..., I, функции формирования множества;

I – число функций, составляющих множество (7);

τ_j – время реализации j-ой, j = 1, 2, ..., J, функции перехвата информативных сигналов ПЭМИН, которая была идентифицирована при оценке этапа реализации угрозы утечки информации;

J – число функций в последовательности идентифицированных функций перехвата ($J \le I$).

Таким образом, временная характеристика γ последовательности идентифицированных функций множества (7) может быть оценена с помощью следующих выражений:

1) при идентификации функции φ_{511} - выражением:

$$\gamma = \overline{\tau}_{511}, \tag{9}$$

где $\overline{\tau}_{511}$ - среднее значение времени реализации функции φ_{511};

2) при идентификации последовательности, состоящей из функций φ_{511} и φ_{512} - выражением:

$$\gamma = M(\tau_{511} \circ \tau_{512}) = \int_{\tau_{511\min}}^{\infty} x \int_{\tau_{512\min}}^{\infty} f_{511}(x-y) \cdot f_{512}(y)\,dy\,dx, \tag{10}$$

где f_{511}, f_{512}, $\tau_{511\min}$ и $\tau_{512\min}$ - плотности распределений и минимальные значения случайных величин τ_{511} и τ_{512}, соответственно, а оператор $M(\cdot)$ означает математическое ожидание от их композиции;

3) при идентификации последовательности, состоящей из функций φ_{511}, φ_{512} и φ_{513} - выражением:

$$\gamma = M(\tau_{511} \circ \tau_{512} \circ \tau_{513}) = \int_{\tau_{511\min}}^{\infty} \int_{\tau_{512\min}}^{y} \int_{\tau_{513\min}}^{z} x \cdot f_{511}(x-y) \cdot f_{512}(y-z) \cdot f_{513}(z)\,dz\,dy\,dx, \tag{11}$$

где φ_{511}, φ_{512}, φ_{513}, $\tau_{511\min}$, $\tau_{512\min}$ и $\tau_{513\min}$ - плотности распределений и минимальные значения случайных величин τ_{511}, τ_{512} и τ_{513}, соответственно;

4) при идентификации последовательности, состоящей из функций f_{511}, φ_{512}, φ_{513} и φ_{521} - выражением:

$$\gamma = M(\tau_{511} \circ \tau_{512} \circ \tau_{513} \circ \tau_{521}) = \int_{\tau_{511\min}}^{\infty} \int_{\tau_{512\min}}^{y} \int_{\tau_{513\min}}^{z} \int_{\tau_{521\min}}^{w} x \cdot f_{511}(x-y) \cdot f_{512}(y-z) \cdot f_{513}(z-w) \cdot f_{521}(w)\,dw\,dz\,dy\,dx, \tag{12}$$

где f_{511}, f_{512}, f_{513}, f_{521}, $\tau_{511\min}$, $\tau_{512\min}$, $\tau_{513\min}$ и $\tau_{521\min}$ - плотности распределений и минимальные значения случайных величин τ_{511}, τ_{512}, τ_{513} и τ_{521}, соответственно;

5) при идентификации последовательности, состоящей из функций φ_{511}, φ_{512}, φ_{513}, φ_{521} и φ_{522} - выражением:

$$\gamma = \overline{\tau}_{511} + \overline{\tau}_{512} + \overline{\tau}_{513} + \overline{\tau}_{521} + \overline{\tau}_{522}, \tag{13}$$

где $\overline{\tau}_{511}$, $\overline{\tau}_{512}$, $\overline{\tau}_{513}$, $\overline{\tau}_{521}$ и $\overline{\tau}_{522}$ - средние значения времени реализации функций φ_{511}, φ_{512}, φ_{513}, φ_{521} и φ_{522}, соответственно;

6) при идентификации последовательности, состоящей из функций f_{511}, φ_{512}, φ_{513}, φ_{521}, φ_{522} и φ_{531} - выражением:

$$\gamma = \overline{\tau}_{511} + \overline{\tau}_{512} + \overline{\tau}_{513} + \overline{\tau}_{521} + \overline{\tau}_{522} + \overline{\tau}_{531}, \quad (14)$$

где $\overline{\tau}_{511}$, $\overline{\tau}_{512}$, $\overline{\tau}_{513}$, $\overline{\tau}_{521}$, $\overline{\tau}_{522}$ и $\overline{\tau}_{531}$ - средние значения времени реализации функций φ_{511}, φ_{512}, φ_{513}, φ_{521}, φ_{522} и φ_{531}, соответственно;

7) при идентификации последовательности, состоящей из функций φ_{511}, φ_{512}, φ_{513}, φ_{521}, φ_{522}, φ_{531} и φ_{532} выражением:

$$\gamma = \overline{\tau}_{511} + \overline{\tau}_{512} + \overline{\tau}_{513} + \overline{\tau}_{521} + \overline{\tau}_{522} + \overline{\tau}_{531} + \overline{\tau}_{532}, \quad (15)$$

где $\overline{\tau}_{511}$, $\overline{\tau}_{512}$, $\overline{\tau}_{513}$, $\overline{\tau}_{521}$, $\overline{\tau}_{522}$, $\overline{\tau}_{531}$ и $\overline{\tau}_{532}$ - средние значения времени реализации функций φ_{511}, φ_{512}, φ_{513}, φ_{521}, φ_{522}, φ_{531}и φ_{532}, соответственно;

Приведенная методика оценки объема информации, раскрываемой в процессе перехвата информативных сигналов ПЭМИН от ОТСС на ОИ является предпосылкой для синтеза адекватной модели распознавания подобного рода угроз информационной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК ЛИТЕРАТУРЫ

1. Скрыль С.В., Никулин С.С. Проблема синтеза моделей распознавания угроз утечки речевой информации по техническим каналам в деятельности органов внутренних дел. Основные положения // Телекоммуникации. – М: «Наука и технологии», 2016. – №4. – С. 24 – 29.

2. Технические средства и методы защиты информации: учебник для студентов высших учебных заведений / С.В. Скрыль, А.А. Шелупанов [и др.]. – М.: Машиностроение, 2008. – 508 с.

3. Информатика: учебник для высших учебных заведений МВД России. – Т. 2. Информатика: Средства и системы обработки данных / С.В. Скрыль, В.А. Минаев, Н.С. Хохлов [и др.]. – М.: Маросейка, 2008. – 544 с.

4. Задача повышения эффективности комплексного технического контроля защищенности речевой информации от утечки по техническим каналам в деятельности объектов промышленно-деловой среды: основные методические положения / С.В. Скрыль, С.С. Никулин, А.В. Щербаков, С.А. Пономаренко // Телекоммуникации. – М: «Наука и технологии», 2016. – №5. – С. 34 – 41.

5. Проблема оптимизации процедур комплексного технического контроля защищенности информации от утечки по каналам ПЭМИН: концепция решения / С.В. Скрыль, В.И. Спивак, А.В. Щербаков, С.А. Пономаренко // Телекоммуникации. – М: «Наука и технологии», 2017. – №10. – С. 23 – 43.