С.В. Зарубин,
кандидат технических наук

Т.Б. Ходырев,
Главное управление вневедомственной охраны МВД России

МАТЕМАТИЧЕСКИЕ МОДЕЛИ ХАРАКТЕРИСТИК ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ В УСЛОВИЯХ ПРОТИВОДЕЙСТВИЯ УТЕЧКЕ ИНФОРМАЦИИ

MATHEMATICAL MODELS OF CHARACTERISTICS OF INFORMATION PROCESSES IN COMPUTER SYSTEMS UNDER CONDITIONS OF COUNTERACTION TO INFORMATION LEAKAGE

Рассматриваются математические модели характеристик и соответствующих показателей процессов утечки информации и противодействия утечке в компьютерных системах (КС). Приводятся аналитические выражения для характеристик информационных процессов в КС в условиях противодействия утечке информации.

Mathematical models of characteristics and corresponding indicators of processes of information leakage and counteraction to leakage in computer networks (CN) are considered. Analytical expressions for characteristics of information processes in CN in conditions of counteraction to information leakage are given.

При исследовании возможностей реализации информационных процессов в компьютерных системах (КС) в условиях противодействия утечке информации важное значение имеет корректность обоснованных характеристик информационных процессов, как комплексных характеристик, отражающих возможности информационных процессов, процессов утечки информации и противодействия утечке.

В соответствии с существующими в современной информатике концептуальными положениями [1] выделяются две основные характеристики информации, как продукта информационной деятельности: ее количество и время реализации информационных процедур. Указанные характеристики описывают и такие специфичные виды информационной деятельности, как перехват (несанкционированное копирование) информации и противодействие утечке информации.

С целью математического представления этих характеристик выделим на множестве состояний X обрабатываемой в КС информации подмножество $Z = \{z_1, z_2, ..., z_L\}$ защищаемых состояний и определим количество защищаемой информации в КС в соответствии с выражением [2]

$$\kappa^{(3)}(Z) = -\sum_{l=1}^{L} p'_l \log_2 p'_l ,$$

в котором p'_l — вероятность обработки состояния z_l.

Аналогичным образом для определения количества перехватываемой (несанкционированно копируемой) информации выделим на множестве состояний Z подмножество $Y = \{y_1, y_2, ..., y_M\}$ состояний, представляющих интерес для злоумышленника, и определим количество перехватываемой (копируемой) злоумышленником информации в процессе

функционирования КС в соответствии с выражением

$$\kappa^{(y)}(Y) = -\sum_{m=1}^{M} p''_m \log_2 p''_m,$$

где p''_m — вероятность перехвата информации состояния y_m.

Временной характеристикой канала утечки информации в КС служит длина временного интервала от момента $t_{(н)}^{(y)}$ начала до момента $t_{(к)}^{(y)}$ окончания перехвата (несанкционированного копирования) информации:

$$\Delta t^{(y)} = t_{(к)}^{(y)} - t_{(н)}^{(y)}.$$

В качестве временной характеристики процесса противодействия утечке информации в КС целесообразно рассматривать длину временного интервала $[t_{(о)}, t_{(п)}]$:

$$\Delta t^{(з)} = t_{(п)} - t_{(о)},$$

где $t_{(о)}$, $t_{(п)}$ — моменты времени обнаружения и подавления канала утечки информации в КС, соответственно.

Показатель возможностей по перехвату (несанкционированному копированию) информации в КС является комплексной характеристикой эффективности канала утечки информации, учитывающей возможности двух разнотипных видов разведки: технической и компьютерной.

Будем полагать, что канал утечки информации в КС функционирует эффективно, если количество $\kappa_i^{(y)}$ перехватываемой (несанкционированно копируемой) информации i-м видом разведки превышает минимальную величину $\kappa_i^{(p)}$, необходимую для раскрытия ее содержания, т.е. при выполнении неравенства

$$\kappa_i^{(y)} \geq \kappa_i^{(p)}. \quad (1)$$

В общем случае обе входящие в неравенство (1) величины являются случайными, поэтому его выполнение является случайным событием.

Вероятность $P(\kappa_i^{(y)} \geq \kappa_i^{(p)})$ характеризует полноту перехватываемой (несанкционированно копируемой) информации i-го вида, обрабатываемой в КС, и может быть использована в качестве частного показателя $a_i^{(y)}$ возможностей по перехвату (несанкционированному копированию) информации в КС, т.е.

$$a_i^{(y)} = P(\kappa_i^{(y)} \geq \kappa_i^{(p)}). \quad (2)$$

По аналогии с изложенным перехват (несанкционированное копирование) информации i-го вида, обрабатываемой в КС, считается реализованным своевременно, если время $\Delta t_i^{(y)}$ перехвата (копирования) информации не превышает время $\tau_i^{(c)}$ ее старения, т.е. при выполнении неравенства

$$\Delta t_i^{(y)} \leq \tau_i^{(c)}. \quad (3)$$

В общем случае обе входящие в неравенство (3) величины — случайные, поэтому его выполнение является случайным событием.

Вероятность $P(\Delta t_i^{(y)} \leq \tau_i^{(c)})$ характеризует своевременность перехвата (несанкционированного копирования) информации i-го вида, обрабатываемой в КС, и может быть использована в качестве частного показателя $b_i^{(y)}$ возможностей по перехвату (несанкционированному копированию) информации в КС, т.е.

$$b_i^{(y)} = P(\Delta t_i^{(y)} \leq \tau_i^{(c)}). \quad (4)$$

В качестве показателя возможностей по перехвату (несанкционированному копированию) информации будем использовать комплексный показатель, учитывающий достоверность и своевременность перехвата (копирования) информации i-го вида, обрабатываемой в КС, в рассматриваемых условиях:

$$e_i^{(y)} = a_i^{(y)} \cdot b_i^{(y)}. \quad (5)$$

С целью аналитического представления показателя (5) рассмотрим его вероятностную интерпретацию относительно производимых злоумышленником попыток перехвата (несанкционированного копирования) информации i-го вида, обрабатываемой в КС, в течение интервала времени Ω исследования информационных процессов в КС.

Интерпретация (2) и (4) как вероятностей попадания соответствующих характеристик в заданный отрезок дает следующее представление (5):

$$e_i^{(y)} = 1 - \left(1 - \prod_{j=1}^{J} a_{ij}^{(y)*} \cdot b_{ij}^{(y)*}\right),$$

где $a_{ij}^{(y)*} = \begin{cases} \dfrac{\kappa_{ij}^{(y)}}{\kappa_{ij}^{(p)}}, & при \quad \kappa_{ij}^{(y)} < \kappa_{ij}^{(p)} \\ 1, & при \quad \kappa_{ij}^{(y)} \geq \kappa_{ij}^{(p)} \end{cases}$;

$b_i^{(y)*} = \begin{cases} 1 - \dfrac{\Delta t_{ij}^{(y)}}{\tau_{ij}^{(c)}}, & при \quad \Delta t_{ij}^{(y)} < \tau_{ij}^{(c)} \\ 0, & при \quad \Delta t_{ij}^{(y)} \geq \tau_{ij}^{(c)} \end{cases}$;

J — число попыток перехвата (несанкционированного копирования) информации i-го вида, обрабатываемой КС, в течение интервала времени Ω;

$\kappa_{ij}^{(y)}$ — количество перехватываемой (несанкционированно копируемой) информации i-м видом разведки в результате j-й, $j = 1, 2, \ldots, J$, попытки перехвата (несанкционированного копирования)

$\kappa_{ij}^{(p)}$ — минимальная величина количества информации i-го вида, необходимая для раскрытия ее содержания в результате j-й, $j = 1, 2, \ldots, J$, попытки перехвата (несанкционированного копирования);

$\Delta t_{ij}^{(y)}$ — длительность j-й, $j = 1, 2, \ldots, J$, попытки перехвата (несанкционированного копирования) информации i-го вида;

$\tau_{ij}^{(c)}$ — время старения информации i-го вида, перехватываемой (несанкционированно копируемой) при j-й попытке перехвата (копирования).

С учетом независимости действий по перехвату и несанкционированному копированию информации, обрабатываемой КС, показатель возможностей по реализации подобного рода действий будет рассчитываться в соответствии с выражением

$$E^{(y)} = 1 - (1 - e_1^{(y)}) \cdot (1 - e_2^{(y)}),$$

где $e_1^{(y)}$ — показатель возможностей по перехвату информации техническими средствами разведки; $e_2^{(y)}$ — показатель возможностей по несанкционированному копированию информации средствами компьютерной разведки.

Исходя из того, что деятельность по защите информации от утечки в КС направлена на противодействие ее перехвату (несанкционированному копированию) при формировании показателя эффективности противодействия, воспользуемся тем же методическим подходом, что и при обосновании показателя возможностей по перехвату (несанкционированному копированию) информации в КС.

Будем полагать, что деятельность по защите информации от перехвата (несанкционированного копирования) в КС i-м видом разведки считается реализованной в полном объеме (обеспечена ее полнота), если обеспечиваемое защитой количество информации $\kappa_i^{(з)}$ не менее минимально допустимой величины $\kappa^{(з)}_{(\min)i}$, т.е. при выполнении неравенства

$$\kappa_i^{(з)} \geq \kappa^{(з)}_{(\min)i}. \qquad (6)$$

Величина $\kappa^{(з)}_{(\min)i}$ минимально допустимого количества информации, обеспечиваемого защитой, определяется характеристиками применяемых в КС средств технической защиты информации и средств защиты от несанкционированного доступа.

В общем случае обе входящие в неравенство (6) величины являются случайными, поэтому его выполнение — случайное событие. Вероятность $P(\kappa_i^{(з)} \geq \kappa^{(з)}_{(\min)i})$ этого события характеризует полноту реализации в КС мер противодействия утечке информации при ее перехвате (несанкционированном копировании) i-м видом разведки и может быть использована в качестве частного показателя $a_i^{(з)}$ эффективности противодействия утечке информации по каналу данного типа, т.е.

$$a_i^{(з)} = P(\kappa_i^{(з)} \geq \kappa^{(з)}_{(\min)i}). \quad (7)$$

Аналогичным образом, меры по противодействию утечке информации при ее перехвате (несанкционированном копировании) i-м видом разведки считаются реализованными своевременно, если время $\Delta t_i^{(з)}$ реагирования на угрозу утечки информации по каналу данного типа не превышает максимально допустимой величины $\tau^{(з)}_{(\max)i}$, т.е. при выполнении неравенства

$$\Delta t_i^{(з)} \leq \tau^{(з)}_{(\max)i}. \quad (8)$$

Максимально допустимая величина времени $\tau^{(з)}_{(\max)i}$ реагирования на угрозу утечки информации по каналу i-го типа в КС определяется характеристиками применяемых средств технической защиты информации и средств защиты от несанкционированного доступа.

Случайный характер входящих в неравенство (8) величин обусловливает его выполнение как случайное событие. Вероятность $P(\Delta t_i^{(з)} \leq \tau^{(з)}_{(\max)i})$ характеризует своевременность реакции на угрозы перехвата (несанкционированного копирования) информации i-м видом разведки в КС и может быть использована в качестве частного показателя $\beta_i^{(з)}$ эффективности противодействия утечке информации по каналу данного типа, т.е.

$$\beta_i^{(з)} = P(\Delta t_i^{(з)} \leq \tau^{(з)}_{(\max)i}). \quad (9)$$

В качестве показателя эффективности противодействия утечке информации по i-му каналу КС будем использовать комплексный показатель, учитывающий полноту и своевременность реакции на угрозы утечки в рассматриваемых условиях:

$$e_i^{(з)} = a_i^{(з)} \cdot \beta_i^{(з)}. \quad (10)$$

С целью аналитического представления показателя (10) рассмотрим его вероятностную интерпретацию относительно мер, принимаемых специалистами по защите информации КС при реагировании на ситуации, связанные с противодействием утечке информации в течение интервала времени Ω исследования информационных процессов в КС.

Интерпретация (7) и (9) как вероятностей попадания соответствующих характеристик в заданный отрезок дает следующее представление (10):

$$e_i^{(з)} = 1 - \left(1 - \prod_{r=1}^{R} a_{ir}^{(з)*} \cdot b_{ir}^{(з)*}\right),$$

где $a_{ir}^{(з)*} = \begin{cases} \dfrac{\kappa_{ir}^{(з)}}{\kappa^{(з)}_{(\min)ir}}, & при \quad \kappa_{ir}^{(з)} < \kappa^{(з)}_{(\min)ir} \\ 1, & при \quad \kappa_{ir}^{(з)} \geq \kappa^{(з)}_{(\min)ir} \end{cases}$;

$$b_{ir}^{(з)*} = \begin{cases} 1 - \dfrac{\Delta t_{ij}^{(з)}}{\tau^{(з)}_{(\max)ir}}, & при \quad \Delta t_{ir}^{(з)} < \tau^{(з)}_{(\max)ir} \\ 0, & при \quad \Delta t_{ir}^{(з)} \geq \tau^{(з)}_{(\max)ir} \end{cases};$$

R — количество мероприятий по реагированию на угрозы утечки информации в КС в течение интервала времени Ω;

$\kappa_{ir}^{(з)}$ — количество информации защищаемое от перехвата (несанкционированного копирования) i-м видом разведки в результате проведения r-го, $r = 1, 2, \ldots, R$, мероприятия;

$\kappa^{(з)}_{(\min)ir}$ — минимально допустимая величина количества информации защищаемого от перехвата (несанкционированного копирования) i-м видом разведки в результате проведения r-го мероприятия;

$\Delta t_{ir}^{(з)}$ — время реагирования на угрозу утечки информации по каналу i-го типа в результате проведения r-го мероприятия;

$\tau^{(з)}_{(\max)ij}$ — максимально допустимая величина времени реагирования на угрозу утечки информации по каналу i-го типа в результате проведения r-го мероприятия.

Исходя из предпосылки, что противодействие утечке информации в КС обеспечивается в случае противодействия утечке информации по техническим каналам и противодействия ее несанкционированному копированию, выражение для показателя эффективности противодействия имеет вид

$$E^{(з)} = e_1^{(з)} \cdot e_2^{(з)}, \quad (11)$$

где $e_1^{(з)}$ — показатель эффективности противодействия утечке информации по техническим каналам; $e_2^{(з)}$ — показатель эффективности противодействия несанкционированному копированию информации.

С целью аналитического представления характеристик информационных процессов в КС в условиях противодействия утечке информации рассмотрим вероятностную интерпретацию группы событий [3], связанных с реализацией информационных процессов в КС, угроз утечки информации и мер противодействия утечке.

Для этого определим следующие события: событие 1 — «Информационный процесс в КС в условиях противодействия утечке информации». Его составляют два события: событие 2 — «Информационный процесс в КС в условиях отсутствия утечки информации» и событие 3 — «Информационный процесс в КС в условиях реализации угроз утечки информации». В свою очередь событие 3 составляют два события: событие 4 — «Меры противодействия утечке информации обеспечивают конфиденциальность информационного процесса» и событие 5 — «Меры противодействия утечке информации не обеспечивают конфиденциальность информационного процесса».

На основе этих событий запишем выражения для характеристик информационного процесса в КС.

Выражение для среднего количества информации, получаемого в результате реализации информационного процесса, имеет вид

$$\bar{\kappa} = \bar{\kappa}_{(пот)} + E^{(у)} \cdot \left(1 - E^{(з)}\right) \cdot \left(\kappa_1^{(у)} \circ \kappa_2^{(у)}\right), \quad (12)$$

где $\bar{\kappa}_{(пот)}$ — среднее значение потенциального количества информации, которое можно получить в результате реализации информационного процесса (в отсутствие угроз утечки информации и мер противодействия утечке); $\kappa_1^{(у)}$ — количество информации, перехватываемой техническими средствами разведки; $\kappa_2^{(у)}$ — количество информации, несанкционированно копируемой средствами компьютерной разведки; $\circ$ — знак композиции случайных величин.

Композиция $\kappa_1^{(у)} \circ \kappa_2^{(у)}$ представляет собой среднее значение количества информации, перехватываемой или несанкционированно копируемой в КС. Данная величина интерпретируется как мера ущерба информационному процессу в единицах количества информации.

Выражение для среднего значения времени Δt реализации информационного процесса имеет вид

$$\Delta \bar{t} = \Delta \bar{t}_{(пот)} + E^{(у)} \cdot \left(1 - E^{(з)}\right) \cdot \left(\Delta t_1^{(у)} \circ \Delta t_2^{(у)}\right), \quad (13)$$

где $\Delta \bar{t}_{(пот)}$ — среднее значение потенциального времени реализации информационного процесса (в отсутствие угроз утечки информации и мер противодействия утечке); $\Delta t_1^{(у)}$ — время перехвата информации техническими средствами разведки; $\Delta t_2^{(у)}$ — время несанкционированного копирования информации средствами компьютерной разведки.

Композиция $\Delta t_1^{(у)} \circ \Delta t_2^{(у)}$ представляет собой среднее значение времени перехвата или несанкционированного копирования информации в КС. Данная величина интерпретируется как мера ущерба информационному процессу в единицах времени реализации информационных процедур.

Очевидно, что левая часть выражений (12) и (13) соответствует событию 1, а слагаемые правой части — его составляющим — событиям 2 и 3 (4 и 5), соответственно.

Таким образом, предложенная в статье событийная интерпретация состояний информационных процессов в КС в условиях противодействия утечке информации дает возможность рассматривать выражения (12) и (13) как аналитические модели соответствующих характеристик информационных процессов.

Полнота представления целевой функции информационных процессов в КС в рассматриваемых условиях позволяет использовать данные модели как инструмент оценки влияния угроз утечки информации по каналам различного вида и мер противодействия утечке на характеристики информационных процессов, и, как следствие, использовать предложенный в статье методический аппарат для обоснования требований к средствам обработки и защиты информации.

ЛИТЕРАТУРА

1. Информатика: учебник для высших учебных заведений МВД России. Т. 1. Информатика: концептуальные основы / В.А. Минаев [и др.]. — М.: Маросейка, 2008. — 464 с.

2. Шеннон К. Математическая теория связи // Работы по теории информации и кибернетике. — М.: ИЛ, 1963.

3. Вентцель Е.С. Теория вероятностей: учебник. — 11-е изд. — М.: КноРус, 2010. — 664 с.