УДК 681. 084

КРИТЕРИИ И ПОКАЗАТЕЛИ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

А.И. Денесюк, А.В. Ивашкин, А.М. Ткачев, К.А. Спорышев
(представил д.т.н., проф. Ю.В. Стасев)

В статье рассматривается ряд критериев качества функционирования системы защиты информации в системах связи и управления.

В настоящее время огромное развитие получили различные системы передачи данных (СПД). Это в первую очередь локальные вычислительные сети (ЛВС). С развитием ЛВС возникает ряд задач, связанных с защитой информации в них. Решение этих задач усложняется воздействием на систему защиты информации (СЗИ) злоумышленика. Наряду с отображением информационных множеств (ИМ) СЗИ должна обеспечивать:

– аутентификацию пользователей;
– секретность передачи информации;
– секретность абонентов и направления соединения;
– протоколирование происходящих в системе событий.

Задачи отображения информационных множеств, обеспечения аутентификации пользователей и секретности передачи информации можно решить посредством применения криптографических преобразований, но для достижения требуемого качественного уровня функционирования СЗИ необходимо разработать некоторые количественные показатели и критерии качества выполнения СЗИ задачи обеспечения целостности и подлинности информации.

Пусть ИС задан априорным алфавитом {А}. Сообщение ИС, состоящее из символов $\mathbf{a_i \in A\ (i=1,N)}$, $\mathbf{N}$ – мощность алфавита, может быть отображено в пространство принятых сообщений $\mathbf{S}$ некоторым решениям $\mathbf{S_j \in S,\ j=\overline{1,M}}$, через пространство криптограмм {У}.

Учитывая воздействие злоумышленика на СЗИ, в пространство принятых сообщений введем функцию $\mathbf{r(a_i, a_r^*, S_j)}$, $\mathbf{i=\overline{1,N}}$, $\mathbf{j=\overline{1,M}}$, $\mathbf{k=\overline{1,L}}$, характеризующую эффективность СЗИ (например, через функцию обмана СЗИ), где $\mathbf{a^*}$ - ложное сообщение, сформированное злоумышленником при передаче сообщения $\mathbf{a_j}$.

В этом случае показатель качества можно определить как математическое ожидание функции $\mathbf{r}$ при реализации всех возможных исходов

$$R = \sum_{i,j,k}^{M,N,K} r\left(a_i, a_k^*, S\right) p(a_i, a_k^*, S_j) \quad . \tag{1}$$

Вероятность $p(a_i, a_k^*, S_j)$ означает вероятность совместной реализации в отдельном испытании события, состоящего в том, что при передаче сообщения a_i, злоумышленник сформировал ложное сообщение a_k^*, и на приемной стороне принято решение S. Вероятность $p(a_i, a_k^*, S_j)$ носит сложный характер, так как отражает случайные факторы воздействия окружающей среды на СЗИ (например, воздействие естественных и принудительных помех в линии связи), а также попытки злоумышленика имитации или подмены сообщения.

Принимая во внимание, что

$$p\left(a_i, a_k^*, S\right) = p(a_i) p\left(S_j / \left(a_i, a_k^*\right)\right), \tag{2}$$

выражение (1) преобразуется к виду

$$r = \sum_{i,j,k}^{M,N,K} r\left(a_i, a_k^*, S\right) p(a_i) p\left(S_j / \left(a_i, a_k^*\right)\right), \tag{3}$$

При C попытках обмана СЗИ, эффективность работы СЗИ описывается выражением (4)

$$r_\Sigma = \sum_{c=1}^{C} \sum_{i,j,k}^{M,N,K} r^c\left(a_i, a_k^*, S\right) p(a_i)\, p\left(S_j / \left(a_i, a_k^*\right)\right), \tag{4}$$

где $r^c\left(a_i, a_k^*, S\right)$ - эффективность средств защиты информации при реализации c - й попытки обмана.

СЗИ принимает решение на основании функции потерь

$$\hat{r} = \min r \tag{5}$$

при условии, что при $i = k$, $r^c(a_i, a_k^*, S) = 0$, так как подменять истинное сообщение истинным злоумышленнику нет смысла (или злоумышленник не влияет на систему).

Таким образом, выражение (5) характеризует средние потери, ожидаемые в СЗИ при реализации отдельных событий. Следовательно, максимальная эффективность системы защиты информации задается условием

$$\min r_{\Sigma} = \min\left\{\sum_{c=1}^{C}\sum_{i,j,k}^{M,N,K} r^{c}(a_i, a_k^{*}, S)p(a_i)p\left(S_j / (a_i, a_k^{*})\right)\right\}. \qquad (6)$$

при $r^{c}(a_i, a_k^{*}, S) = 0$, если $i = k$.

В соответствии с выработанными критериями оценки подлинности и целостности информации, среднее значение вероятности обмана при реализации всех возможных сообщений имеет вид

$$P_{\text{обмана}} = \sum p(a_i) p_{\text{р.у.обм}} p_{\text{вз.сс}} p_{\text{вс.п.к.}}. \qquad (7)$$

Рассмотрим подробно значение вероятностей, входящих в (7). В рассматриваемой модели неверное отображение переданного сообщения в множество принятых рассматривается как успешная реализация угрозы обмана системы, вероятность которой $p_{\text{р.у.обм.}}$ зависит от возможности реализации таких случайных событий как обман системы за счет ошибок в канале передачи данных ($p_{\text{обм.кс.}}$), обмана системы злоумышленником путем подмены ($p_{\text{под.}}$) или имитации ($p_{\text{им.}}$) переданных сообщений, а также обмана системы несанкционированными действиями пользователей ($p_{\text{н.д.п.}}$), таким как уничтожение сообщения ($p_{\text{ус.}}$) или его подмены ($p_{\text{п.}}$). Таким образом, вероятность обмана системы защиты информации зависит от успешной реализации угроз искажения информации в канале связи, успешной имитации или подмены сообщений злоумышленником, и успешного искажения информации несанкционированными пользователями. В рассматриваемой модели угроз злоумышленник с вероятностью, равной единице осуществляет либо подмену, либо имитацию сообщения, т.е.

$$p_{\text{обм.}} = p_{\text{обм.кс.}} + (p_{\text{под.}} + p_{\text{им.}}) + (p_{\text{у}} + p_{\text{нп.}}),$$

Вероятность успешной имитации или подмены сообщения ($p_{\text{под}} + p_{\text{им}}$) злоумышленником будем описывать выражением

$$(1 - p_{\text{ош.}})\,[p_{\text{под.}} p_{\text{ус.под.}} + (1 - p_{\text{под.}}) p_{\text{ус.им.}}], \qquad (8)$$

где $p_{\text{ош.}}$ – вероятность, характеризующая качество канала связи, зависит от энергетических характеристик канала, метода обработки сигналов и используемых методов помехоустойчивого кодирования.

Важной характеристикой функционирования СЗИ является вероятность обмана системы за счет ошибок в канале передачи данных ($p_{\text{обм.кс.}}$), который будем вычислять, используя выражение

$$P = \{1 - [p_{\text{под.}} p_{\text{ус.под.}} + (1 - p_{\text{под.}})\, p_{\text{ус.под.}}]\} p_{\text{ош.}}$$

Вероятность подмены сообщения $\mathbf{P_{ус.под.}}$ зависящая от успешного преобразования одной криптограммы в другую, а также от формирования цифровой подписи $\mathbf{Z_i}$ к криптограмме $\mathbf{Y_i}$, описывается выражением

$$\mathbf{P_{ус.им.} = P(Y_i)\ P(Y_i / Z_i)}, \qquad (9)$$

где $\mathbf{P(Y_i / Z_i)}$ – вероятность формирования разрешенной цифровой подписи к криптограмме $\mathbf{Y_i}$.

В случае передачи открытого, подписанного цифровой подписью, сообщения $\mathbf{P(Y_i) = 1}$ и выражение (9) имеет вид

$$\mathbf{P_{ус.под.} = P(a_i / Z_i)}. \qquad (10)$$

При реализации угрозы имитации выражение для $\mathbf{P_{ус.им.}}$, по аналогии с (8), имеет вид

$$\mathbf{P_{ус.им.} = P(Y_i)P(Y_i / Z_i)}. \qquad (11)$$

Под вероятностью отказа будем понимать вероятность события, состоящего в том, что получатель сообщения уничтожает его, а также несанкционированно уничтожает документацию, регистрирующую ее поступление. Исследования показали, что $\mathbf{P_{отказа}}$ зависит от степени защиты узла СЗИ от несанкционированного доступа и определяется выражением

$$\mathbf{P_{отказа} = \prod_{r=1}^{R} P_r}\ , \qquad (12)$$

где $\mathbf{P_r}$ – вероятность преодоления $\mathbf{r}$ уровня защиты от НСД.

Под вероятностью несанкционированной подмены будем понимать вероятность события, состоящего в том, что получатель сообщения подменит его другим, а регистрирующую документацию уничтожит, т.е.

$$\mathbf{P_{НП} = P_{iП} \prod_{r=1}^{R} P_r}\ , \qquad (13)$$

где $\mathbf{P_{in}}$ - вероятность подмены $\mathbf{i}$ - го сообщения.

Вероятность $\mathbf{P_{вс.п.с.}}$ – вероятность вскрытия системы при перехвате символов ключа. Определим $\mathbf{P_{вс.п.с.}}$ как $\mathbf{L_{min} / L_п}$, где $\mathbf{L_{min}}$ - минимально необходимое количество символов ключа для того, чтобы вскрыть систему (расстояние единственности), $\mathbf{L_п}$ - количество перехваченных символов ключа. Будем считать, что $\mathbf{L_п = D}$ длиннее ключа.

Из теории информации известно, что для определения $\mathbf{L_{min}}$ используется следующее выражение

$$\mathbf{L_{min} = H(K) / 2 \log_2 N}\ , \qquad (14)$$

где $\mathbf{H(K)}$ – энтропия источника ключей, которая определяется как

$$H(K) = \sum_{i=1}^{D^N} P(K_i) \log_2 P(K_i) . \qquad (15)$$

После подстановки (13) в (14) получим

$$P_{вс.п.с.} = \frac{\sum_{i=1}^{D^N} P(K_i) \log_2 P(K_i)}{2 \log_2 ND} .$$

После подстановки (8), (9), (10) в (7) получим выражение, которое в наиболее общей форме описывает и учитывает все модели угроз, возможные со стороны злоумышленника, а также качество канала связи и несанкционированные действия пользователей.

$$P_{об} = \sum p(a)\Big\{\big(1-p_{ош}\big)\Big[p_{под}P(Y_i)P\big(Y_i/Z_i\big)+\big(1-p_{под}\big)P(Y_i)P\big(Y_i/Z_i\big)\Big]+$$
$$+\Big\{1-\Big[p_{под}P(Y_i)P\big(Y_i/Z_i\big)+\big(1-p_{под}\big)P(Y_i)P\big(Y_i/Z_i\big)\Big]\Big\}p_{ош}+$$
$$+\Big\{1-\Big\{\big(1-p_{ош}\big)\Big[p_{под}P(Y_i)P\big(Y_i/Z_i\big)+\big(1-p_{под}\big)P(Y_i)P\big(Y_i/Z_i\big)\Big]+$$
$$+\Big\{1-\Big[p_{под}P(Y_i)P\big(Y_i/Z_i\big)+\big(1-p_{под}\big)P(Y_i)P\big(Y_i/Z_i\big)\Big]\Big\}p_{ош}\Big\}\cdot$$

$$\cdot\prod_{r=1}^{R}P_r+\Big\{1-\Big\{\big(1-p_{ош}\big)\Big[p_{под}P(Y_i)P\big(Y_i/Z_i\big)+\big(1-p_{под}\big)P(Y_i)P\big(Y_i/Z_i\big)\Big]+$$
$$+\Big\{1-\Big[p_{под}P(Y_i)P\big(Y_i/Z_i\big)+\big(1-p_{под}\big)P(Y_i)P\big(Y_i/Z_i\big)\Big]\Big\}p_{ош}\Big\}\Big\}P_{НП}\prod_{r=1}^{R}P_r .$$

Таким образом, совокупность введенных показателей позволяет в полной мере оценить целостность и подлинность информации, циркулирующей в ИС «GLOBALSTAR».

ЛИТЕРАТУРА

1. Кузьмин И.В., Кедрус В.А. Основы теории информации и кодирования. – К.: Вища школа, 1986. – 320 с.

2. Работы по теории информации и кибернетике. – М.: Иностранная литература, 1963. – 428 с.

3. Горбенко И.Д., Стасев Ю.В. Безопасность информации в космических системах связи и управления // Космічна наука і технологія.- 1996. - Т2. - №5 - 6. - С.64 - 68.