

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) злоумышленника. 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 $\{A\}$. Сообщение ИС, состоящее из символов $a_i \in A$ ($i = \overline{1, N}$), N – мощность алфавита, может быть отображено в пространство принятых сообщений S некоторым решением $S_j \in S$, $j = \overline{1, M}$, через пространство криптограмм $\{U\}$.

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

В этом случае показатель качества можно определить как математическое ожидание функции r при реализации всех возможных исходов

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

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 злоумышленника имитации или подмены сообщения.

Принимая во внимание, что

$$p(a_i, a_k^*, S) = p(a_i) p(S_j / (a_i, a_k^*)), \quad (2)$$

выражение (1) преобразуется к виду

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

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

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

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

СЗИ принимает решение на основании функции потерь

$$\hat{r} = \min r \quad (5)$$

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

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

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

$$P_{\text{обмана}} = \sum p(a_i) p_{p.y.obm} p_{вз.сц} p_{вс.п.к}. \quad (7)$$

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 $p_{p.y.obm}$ зависит от возможности реализации таких случайных событий как обман системы за счет ошибок в канале передачи данных ($p_{обм.кс.}$), обмана системы злоумышленником путем подмены ($p_{под.}$) или имитации ($p_{им.}$) переданных сообщений, а также обмана системы несанкционированными действиями пользователей ($p_{н.д.п.}$), таким как уничтожение сообщения ($p_{ус.}$) или его подмены ($p_{п.}$). 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.

$$P_{обм.} = P_{обм.кс.} + (p_{под.} + p_{им.}) + (p_y + p_{пп.}),$$

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

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

где $p_{ош.}$ – 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 ($p_{обм.кс.}$), который будем вычислять, используя выражение

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

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

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

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

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

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

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

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

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 $P_{\text{отказа}}$ зависит от степени защиты узла СЗИ от несанкционированного доступа и определяется выражением

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

где P_r – вероятность преодоления 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.

$$P_{\text{НП}} = P_{\text{иП}} \prod_{r=1}^R P_r, \quad (13)$$

где $P_{\text{иП}}$ - вероятность подмены i -го сообщения.

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

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

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

где $H(K)$ – энтропия источника ключей, которая определяется как

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

После подстановки (13) в (14) получим

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

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.

$$\begin{aligned} P_{\text{об}} = & \sum P(a) \left\{ (1 - p_{\text{ош}}) [p_{\text{под}} P(Y_i) P(Y_i/Z_i) + (1 - p_{\text{под}}) P(Y_i) P(Y_i/Z_i)] + \right. \\ & + \left\{ 1 - [p_{\text{под}} P(Y_i) P(Y_i/Z_i) + (1 - p_{\text{под}}) P(Y_i) P(Y_i/Z_i)] \right\} p_{\text{ош}} + \\ & + \left\{ 1 - \left\{ (1 - p_{\text{ош}}) [p_{\text{под}} P(Y_i) P(Y_i/Z_i) + (1 - p_{\text{под}}) P(Y_i) P(Y_i/Z_i)] \right\} + \right. \\ & \left. \left. + \left\{ 1 - [p_{\text{под}} P(Y_i) P(Y_i/Z_i) + (1 - p_{\text{под}}) P(Y_i) P(Y_i/Z_i)] \right\} p_{\text{ош}} \right\} \right\} \cdot \\ & \cdot \prod_{r=1}^R P_r + \left\{ 1 - \left\{ (1 - p_{\text{ош}}) [p_{\text{под}} P(Y_i) P(Y_i/Z_i) + (1 - p_{\text{под}}) P(Y_i) P(Y_i/Z_i)] \right\} + \right. \\ & \left. + \left\{ 1 - [p_{\text{под}} P(Y_i) P(Y_i/Z_i) + (1 - p_{\text{под}}) P(Y_i) P(Y_i/Z_i)] \right\} p_{\text{ош}} \right\} P_{\text{НП}} \prod_{r=1}^R P_r. \end{aligned}$$

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.