НАУКОВО – ТЕХНІЧНИЙ ЖУРНАЛ "ЗАХИСТ ІНФОРМАЦІЇ" №4, 2004
УДК 681.5.015: 004.056.57
Маракова И.И.

ПОЛУСЕКРЕТНЫЕ СИСТЕМЫ С ЦИФРОВЫМИ ВОДЯНЫМИ ЗНАКАМИ В УСЛОВИЯХ РАЗЛИЧНЫХ СЦЕНАРИЕВ АТАКИ АДДИТИВНЫМ ШУМОМ

Последнее время стали появляться публикации о применении технологий цифровых водяных знаков (ВЗ) при решении задач *защиты IP протоколов* в Интернете. Действительно, представляется значительно упростить логические структуры данных протоколов посредством применения идентификации и аутентификации с помощью ВЗ [1]. В данном случае секретная структура системы с ВЗ, когда пользователь должен знать секретный ключ, а именно — ВЗ, не совсем приемлема [2, 3].

Термин *полусекретная* употребляется для обозначениия такой структуры системы, когда в детекторе обнаружение ВЗ происходит без СК, но удаление ВЗ без СК не возможно. Именно такая структура, когда для обнаружения ВЗ никакой дополнительной информации не требуется, но удалить ВЗ без специальных знаний нельзя, весьма интересна на практике для Интернет–приложений.

Представим ВЗ в виде

$$w(\bar{n}) = \Delta(\bar{n})l(\bar{n}), \quad \bar{n} \in A_N, \tag{1}$$

где $l(\bar{n})$— случайная величина с заданными вероятностными мерами и являющаяся СК $, l(\bar{n}) \in L;$

$\Delta(\bar{n}) = \pm 1$ — псевдослучайная последовательность с равномерным распределением;

$\bar{n} = n_1 n_2, \ n_1 = 1,...,N_1, \ n_2 = 1,...,N_2, \ N = N_1 N_2$— число пикселей, если основное покрывающее сообщение $c(n)$ (ОПС) является изображением.

До добавления помехи в стегасообщение $s(\bar{n}) = c(\bar{n}) + w(\bar{n}) = c(\bar{n}) + \Delta(\bar{n})l(\bar{n})$, $\bar{n} \in A_N$, любой пользователь может оценить функционал неинформированного линейного корреляционного детектора (ЛКД) $\Lambda = f(s(\bar{n}), \Delta(\bar{n}))$, $\bar{n} \in A_N$, который при наличии ВЗ

$$\Lambda_1 = f((c(\bar{n}) + \Delta(\bar{n})l(\bar{n})), \Delta(\bar{n})) = \sum_{\bar{n} \in A_N} c(\bar{n})\Delta(\bar{n}) + \sum_{\bar{n} \in A_N} l(\bar{n}), \ \bar{n} \in A_N, \tag{2}$$

а при отсутствии

$$\Lambda_0 = (c(\bar{n}) + \Delta(\bar{n})) = \sum_{\bar{n} \in A_N} c(\bar{n})\Delta(\bar{n}), \ \bar{n} \in A_N. \tag{3}$$

Математические ожидания функционала ЛКД

$$E(\Lambda_1) = \sum_{\bar{n} \in A_N} E(l(\bar{n})) = NE(L), \ E(\Lambda_0) = 0, \tag{4}$$

что позволяет надеяться на успешное детектирование ВЗ при неизвестном ОПС.

Стегасообщение после атакующих преобразований в виде аддитивного шума

$$s'(\bar{n}) = c(\bar{n}) + w(\bar{n}) + \varepsilon(\bar{n})$$

Поскольку $\Delta(\bar{n})$ известно всем пользователям, то возможно создание помехи $\varepsilon(\bar{n}) = -l'(\bar{n})\Delta(\bar{n})$, т.е. $s'(\bar{n}) = c(\bar{n}) + \Delta(\bar{n})l(\bar{n}) - l'(\bar{n})\Delta(\bar{n})$, $\bar{n} \in A_N$.

При наличии ВЗ на выходе детектора легального пользователя

$$\Lambda_1 = \sum_{\bar{n} \in A_N} (\Delta(\bar{n})l(\bar{n}) - \Delta(\bar{n})l'(\bar{n}))l(\bar{n})\Delta(\bar{n}) = \sum_{\bar{n} \in A_N} (l^2(\bar{n}) - l(\bar{n})l'(\bar{n})), \tag{5}$$

а при отсутствии ВЗ

$$\Lambda_0 = -\sum_{\bar{n}\in A_N} l'(\bar{n})l(\bar{n}), \tag{6}$$

где математические ожидания функционала ЛКД

$$E(\Lambda_1) = N(E(L^2) - E(L')E(L), \quad E(\Delta_0) = -NE(L)E(L').$$

Поскольку $L \geq 0,\ L' > 0,$ то $E(L^2) > E(L)E(L')$. Для равномерного распределения L в интервале $\{0,\ \alpha\}$ получим

$$E(\Lambda_1^2) = Var(\Lambda_1) = \frac{N}{12}\alpha^2. \tag{7}$$

С другой стороны, поскольку $E(\Lambda_0) < 0$ т.е. гипотезы являются априорно различимы, но атакующий может заранее обнаружить ВЗ и сформировать помеху в виде $\varepsilon(\bar{n}) = -l'(\bar{n})\Delta(\bar{n}),\ \bar{n} \in A_N$, а при отсутствии ВЗ не создавать никакой помехи. Тогда $E(\Lambda_0) = 0$, что также не желательно.

Рассмотрим более подробно сценарий создания помехи $\varepsilon(\bar{n}) = \alpha\Delta(\bar{n})$, когда $\Lambda_0 = \alpha \sum_{\bar{n}\in A_N} \Delta(\bar{n})$ и $E(\Lambda_0) > 0$. При детектировании ВЗ без ключа по правилу (3.30), (3.31) Λ_1 и Λ_0 можно считать случайными гауссовыми величинами, причем $E(\Lambda_1) = NE(L)$ и $E(\Lambda_0) = 0$. Если предположить для конкретизации, что величина L равномерно распределена на интервале $(0, \alpha)$. Тогда из (3.30), (3.31) получим

$$E(\Lambda_1) = \frac{\alpha}{2}N,\ Var\Lambda_0 = \sigma_c^2 N,\ Var\Lambda_1 = (\sigma_c^2 + \alpha^2/12)N. \tag{8}$$

Используя решающее правило: $\Lambda \leq \lambda$ — нет ВЗ, $\Lambda \geq \lambda$ — есть ВЗ, получим следующее выражение для вероятностей ошибок

$$P_m = 1 - Q\frac{(\lambda - \frac{\alpha}{2}N)}{\sqrt{(\sigma_c^2 + \frac{\alpha^2}{12})N}} = 1 - Q((\lambda_0 - \frac{\alpha}{2})\sqrt{\frac{N}{\sigma_c^2 + \frac{\alpha^2}{12}}}), \tag{9}$$

$$P_{fa} = Q\frac{\lambda}{\sqrt{(\sigma_c^2 + \frac{\alpha^2}{12})N}} = Q(\lambda_0\sqrt{\frac{N}{\sigma_c^2 + \frac{\alpha^2}{12}}}), \tag{10}$$

где $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{t^2}{2}}dt$

Если задано отношение сигнал/шум при погружении ВЗ $\eta_w = \frac{\sigma_c^2}{Var(\Delta L)}$, то при $Var(\Delta L) = E(L^2)E(\Delta^2) = E(L^2)$, равномерном распределении L на интервале $(0,\ \alpha)$ получим $Var(\Delta l) = \frac{\alpha^3}{3}$ и $\eta_w = \frac{3\sigma_c^2}{\alpha^2}$, что является ограничением на значение α. Тогда (9), (10) преобразуются к виду

$$P_m = 1 - Q(\lambda_0' - \frac{1}{2})\sqrt{\frac{N}{\frac{\sigma_c^2}{\alpha^2} + \frac{1}{12}}} = 1 - Q(\lambda_0' - \frac{1}{2})\sqrt{\frac{N}{\frac{\eta_w}{3} + \frac{1}{12}}} = 1 - Q((2\lambda_0' - 1)\sqrt{\frac{3N}{4\eta_w + 1}})$$

$$P_{fa} = 4Q(2\lambda_0'\sqrt{\frac{3N}{4\eta_w + 1}}). \qquad (12)$$

При $\eta_w = \eta_\alpha$ (11), (12) весьма близки с аналогичными формулами для секретных систем с ВЗ [3]..Таким образом, переход от секретных к полусекретным системам с ВЗ не вносит существенного ухудшения в эффективность системы без атакующих преобразований.

Рассмотрим сценарий, когда после обнаружения ВЗ в канале атакующего осуществляются преобразования, преследующие целью устремить для детектора легального пользователя $P_{fa} \approx P_m \to \infty$. Естественной атакой в этом случае является формирование помехи вида $\varepsilon(\bar{n}) = -\Delta(\bar{n})l'(\bar{n})$, $\bar{n} \in A_N$. Хотя атакующему не известно в точности $l(\bar{n})$, т.е полная компенсация не возможна, но при известном $\Delta(n)$ и то, что $l(n) \geq 0$ атака может быть весьма эффективной. Функционал информированного детектора легального пользователя

$$\Lambda = \Lambda_l = \sum_{n \in A_N} (l^2(\bar{n}) - l'(\bar{n})l(\bar{n})), \qquad (13)$$

причем

$$E(\Lambda_l) = N(E(L^2) - E(L')E(L)), Var(\Lambda_l) = E(\Lambda_l^2) - (E(\Lambda_l))^2. \qquad (14)$$

Если предположить, что L' и L характеризуются одинаковыми плотностями распределения, то $E(\Lambda^2) = \frac{\alpha^2}{3}$, $E(L) = \frac{\alpha}{2}$, $E(L') = \frac{\alpha}{2}$, $E(\Lambda_l) = (\frac{\alpha^2}{3} - \frac{\alpha^2}{4})N = N\frac{\alpha^2}{12}$,

$$E(\Lambda^2{}_l) = E((L^2 - L'L)^2) = E(L^4) - 2E(L')E(L^3) + E((L'))E(L^2) = \frac{11}{180}\alpha^4, Var\Lambda_l =$$

$$= N(\frac{11}{180}\alpha^4 - \frac{\alpha^4}{144}) = N\alpha^4\frac{13}{240}$$

Рассмотрим атаку в случае отсутствия ВЗ, что не известно для нелегальных пользователей. Если атакующий сформировал такую же помеху, как и при наличии ВЗ, $\varepsilon(\bar{n}) = -\Delta(\bar{n})l'(\bar{n})$, $\bar{n} \in A_N$ то функционал ЛКД $\Lambda_0 = -\sum_{n \in A_N} l'(\bar{n})l(\bar{n})$ и поскольку $\Lambda_0 \leq 0$, такая помеха не эффективна для атаки. Оптимальной для атакующего в этом случае будет помеха $\varepsilon(\bar{n}) = l'(\bar{n})l(\bar{n}), \bar{n} \in A_N$, которая имитирует присутствие ВЗ. Тогда функционал ЛКД легального пользователя, $\Lambda_0 = \sum_{n \in A_N} l'(\bar{n})l(\bar{n})$, где диапазон равномерно распределенной величины L' исходя из допустимого критерия верности ВЗ сузится за счет помехи и станет $(0, \alpha')$, т.е. $E(\Lambda_0) = N(\frac{\alpha'}{2}\frac{\alpha}{2}) = N\frac{\alpha\alpha'}{4}$. Если $\alpha = \alpha'$, то $E(\Lambda_l) < E(\Lambda_0)$ и обнаружение будет не эффективным. На практике более реально соотношение $\alpha \neq \alpha'$. Тогда из (3.43) $E(\Lambda_l) = N(\frac{\alpha^2}{3} - \frac{\alpha}{2}\frac{\alpha'}{2}) = N\alpha(\frac{\alpha}{3} - \frac{\alpha'}{4})$. Условие надежного восприятия при

погружении ВЗ $\frac{\alpha^2}{12} < \rho$ и после атаки $\frac{\alpha^2}{12} + \frac{\alpha'^2}{12} \le \rho'$, причем $E(\Lambda_0) = N(\frac{\alpha}{2}\frac{\alpha'}{2}) = N\alpha\alpha'$. Очевидно, что если $\alpha << \alpha'$, то детектирование ВЗ представляется возможным, а если $\alpha = \alpha'$ ($\rho' = 2\rho$) — не возможным в отличие от секретных систем с ВЗ. Поэтому данная структура может претендовать на реализуемость только при дополнительных, например, протокольных усложнениях.

Рассмотрим еще один вариант построения полусекретной системы при использовании периодических ПСП. В этом случае сигнал после погружения определится как $w(\bar{n}) = \alpha v(\bar{n})$, $\bar{n} \in A_N$, где $v(\bar{n}) \pm 1$ является периодическим сигналом с периодом $N_0 < N$ при погружении ВЗ в конкретные пиксели ОПС —маску. Если каждому из пользователю известна размерность фрагментов ОПС, куда погружаются периодов ПСП ВЗ, то функционал ЛКД

$$\Lambda = \sum_{j \in J} \sum_{\substack{\bar{n}_i \in A_{Tj} \\ \bar{n}_{i'} \in A_{Tj}}} s(\bar{n}_i) s(\bar{n}_{i'}),$$

где A_{Tj} — фрагменты ОПС с периодами ПСП ВЗ, $j = 1,2..., J$.

Если предположить, что периоды ВЗ достаточно разнесены друг от друга, то $E(\Lambda_1) = \alpha^2 N > 0$, а при отсутствие ВЗ $E(\Lambda_0) = 0$, т.е. детектирование ВЗ становится возможным, причем без знания пользователями последовательности $l(\bar{n})$, $\bar{n} \in A_N$.

Рассмотрим сценарий атаки по следующему алгоритму. Атакующий знает позиции, в которых расположены периодические последовательности, но не знает значений $v(\bar{n})$, $\bar{n} \in A_N$. Целью атаки является удаление ВЗ после несанкционированного детектирования или устремление $P_{fa} \approx P_m \to \infty$ для детектора легального пользователя. В случае отсутствия ВЗ в стегасообщении атакующий попытается создать ложные ВЗ. Функционал детектора легального пользователя $\Lambda_1 = \sum_{\bar{n} \in A_N} s'(\bar{n}) v(\bar{n})$ формируется на всех фрагментах с периодическими ВЗ, т.е для информированного ЛКД $\Lambda_1 = \sum_{j \in J} \sum_{\bar{n}_j \in A_{Tj}} (\alpha v(\bar{n}_j) + \varepsilon(\bar{n}_j) v(\bar{n}_j))$.

При таком сценарии эффективными действиями атакующего является создание аддитивной помехи [3]. Тогда при отсутствие ВЗ функционал детектора легального пользователя $\Lambda_0 = \sum_{j \in J} \sum_{\bar{n}_j \in A_j} (\varepsilon(\bar{n}_j) v(\bar{n}_j))$.

Если $Var(\Lambda_1) = Var(\Lambda_0)$, то в частном случае наличия только двух периодов при независимости помехи на каждом из них $Var(\Lambda_1) = Var(\Lambda_0) = N_0 \sigma_\varepsilon^2$, где $\sigma_\varepsilon^2 = Var(\varepsilon(\bar{n}))$. При повторении атакующим помехи на втором периоде, то $Var(\Lambda_1) = Var(\Lambda_0) = 4\frac{N_0}{2}\sigma_\varepsilon^2 = 2N_0\sigma_\varepsilon^2$, т.е. оказывается больше и поэтому такой алгоритм более эффективен для атаки. Для рассматриваемого сценария атаки

$$P_m = 1 - Q((\lambda_0' \eta_\alpha - 1) \sqrt{\frac{N\eta_w}{2(\eta_\alpha - \eta_w)}}), \qquad (15)$$

$$P_{fa} = Q\left(\frac{\lambda'_0}{\rho}\right)\sqrt{\frac{N\eta_w}{\eta_\alpha - \eta_w}} \tag{16}$$

Таким образом, данный метод построения полусекретных систем ВЗ представляется более предпочтительным, чем рассмотренный выше, однако, в предположении независимости фрагментов $c(\bar{n})$, $\bar{n} \in A_N$ для двух периодов в частном случае и всех — в общем случае численные исследования эффективности полусекретных систем с ВЗ требуют уточнения структуры, т.е. конкретизации заданных условий и ограничений. Функционал детектора любого пользователя полусекретной системы

$$\Lambda = \sum_{n=1}^{N} s(n)w(n) = \sum_{n=1}^{N} s(n)\Delta(n) = \begin{cases} \Lambda_1 = \sum_{n=1}^{N} (c(n) + \Delta(n)l(n))\Delta(n), & \textbf{\textit{при наличии ВЗ,}} \\ \Lambda_0 = \sum_{n=1}^{N} c(n)\Delta(n), & \textbf{\textit{при отсутствии ВЗ,}} \end{cases}$$

вероятности ошибок в общем случае [3]

$$P_m = 1 - Q\left(\frac{\lambda - E(\Lambda_1)}{\sqrt{Var\,\Lambda_1}}\right) \tag{17}$$

$$P_{fa} = Q\left(\frac{\lambda - E(\Lambda_0)}{\sqrt{Var\,\Lambda_0}}\right) \tag{18}$$

где $E(\Lambda_0) = 0$, $E(\Lambda_1) = NE(\Delta(n)l(n)) = \frac{ND}{2}$, $Var\,\Lambda_0 = Var\Lambda_1 = N\sigma_c^2$, $D^2 = Var(\Delta(n)l(n))$

В условиях аддитивного шума атакующего канала и с учетом того, что атакующему известно $\Delta(n)$, $n \in A_N$ логично предположить

$$\begin{cases} \varepsilon(n) = \sigma_\varepsilon \Delta(n) \text{ при отсутствие } ВЗ, \\ \varepsilon(n) = 0 \text{ при присутствие } ВЗ. \end{cases} \tag{19}$$

и, соответственно, для ЛКД любого пользователя

$$\begin{cases} E(\Lambda') = E(\Lambda'_0) = N\sigma_\varepsilon & \text{при отсутствие ВЗ,} \\ E(\Lambda') = E(\Lambda'_1) = \frac{ND}{2} & \text{при присутствие ВЗ.} \end{cases} \tag{20}$$

С учетом данной стратегии необходимо внести изменение и в формировании параметров искажений

$$\eta_a = \frac{Var(c(n))}{Var(\varepsilon(n))} = \frac{\sigma_c^2}{\sigma_\varepsilon{}^2}, \tag{21}$$

откуда

$$\sigma_\varepsilon = \sqrt{\frac{\sigma_c^2}{\eta_a}} \tag{22}$$

С другой стороны, если ВЗ погружены, то

$$D = \sqrt{\frac{3\sigma_c^2}{\eta_w}} \tag{23}$$

Поскольку атака аддитивным шумом применяется только в условиях отсутствия ВЗ, то

$$E(\Lambda'_0) = N\sigma_\varepsilon = N\sqrt{\frac{\sigma_c^2}{\eta_a}} \tag{24}$$

$$E(\Lambda'_1) = N\frac{D}{2} = N\sqrt{\frac{3\sigma_c^2}{4\eta_a}} \tag{25}$$

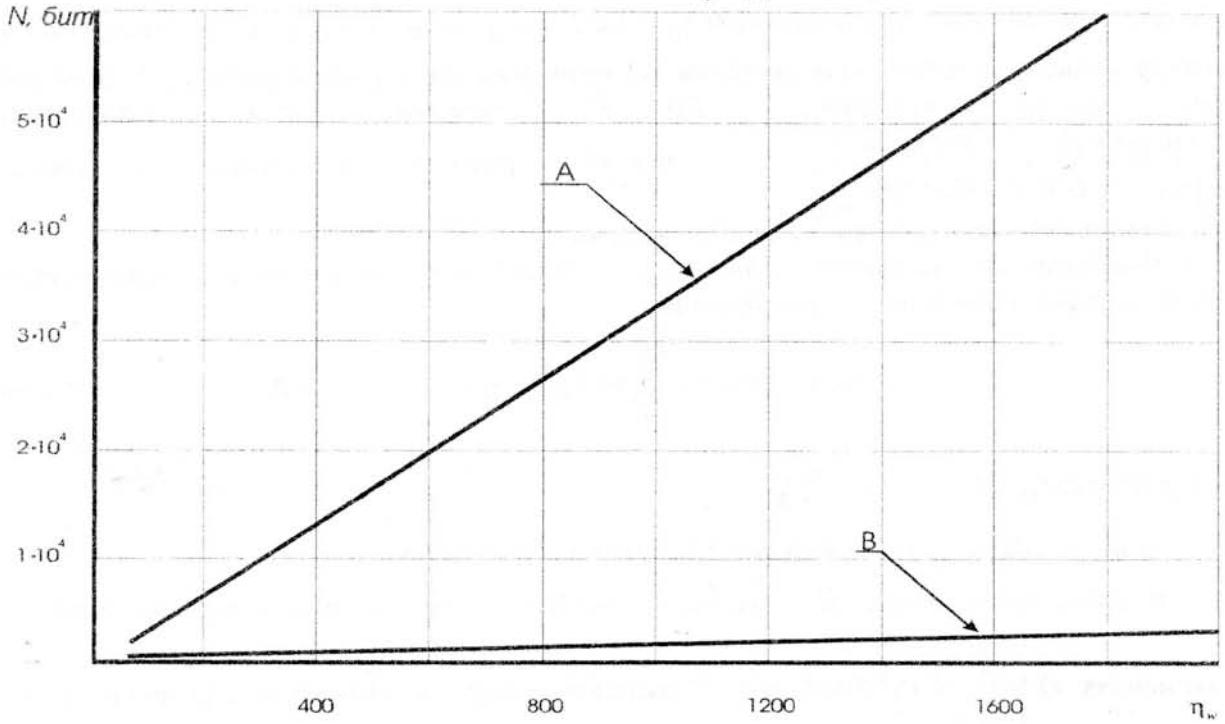

Рис.1. Зависимость числа бит ВЗ N от величины η_W для случаев $\eta = \eta_w/\eta_\alpha = 1{,}1$ при использовании легальным пользователем неинформированного детектора (А), информированного детектора (В) в условиях атаки аддитивным шумом при отсутствие ВЗ и выполнении соотношения $P_{fa}=10^{-3}$

Численный анализ описанного сценария действий нелегального пользователя при информированном и неинформированном детекторе легального пользователя (рис.1) продемонстрировал несущественные отличия от аналогичных структур секретной системы [3].

Если нелегальный пользователь точно знает о факте присутствия или отсутствия ВЗ, то возможно применение следующее стратегии фальсификации ВЗ при отсутствие ВЗ

$$\begin{cases} \varepsilon(n) = \varepsilon_0(n) = \sigma_\varepsilon e(n) \ \textit{при отсутствие ВЗ}, \\ \varepsilon(n) = \varepsilon_1(n) = -l'(n)\Delta(n) \ \textit{при присутствие ВЗ}., \end{cases}$$

где $l'(n)$, $n \in A_N$ является равномерной ПСП в диапазоне $\{0,\ D'\}$.

Функционалы ЛКД легального пользователя Λ'' после описаного сценария атакующего характеризуются следующими вероятностными мерами

$$E(\Lambda'') = E(\Lambda''_0) = \sigma NE(l(n)) = \frac{\sigma_\varepsilon ND}{2} = N\frac{\sigma_c^2}{\eta_w}\sqrt{\frac{3}{4}}$$

$$E(\Lambda'') = E(\Lambda''_1) = N(E(L^2)) - E(l(n)E(l'(n)) = N(\frac{D^2}{3} - \frac{DD'}{4}) = N(\frac{\sigma_c^2}{\eta_w} - \sqrt{\frac{3\sigma_c^2}{16}}D')$$

из сравнения которых очевидно $E(\Lambda_0'') < E(\Lambda''_1)$ и, следовательно, правильное детектирование легальным пользователем ВЗ возможно только при больших D' является очень малой величиной. Другими словами, если выполняется $\frac{Var(c(n))}{Var(w(n)+\varepsilon(n))} \approx \frac{Var(c(n))}{Var(w(n))}$, что лишено практического смысла в рамках рассматриваемого сценария действий атакующего.

Выходом для легального пользователя может быть использование следующего подхода при формировании стегасообщения

$$s(n) = c(n) + \sum_{l}^{L} w_l(n), \quad n = 1, 2, \ldots, LN_0, \tag{26}$$

где $w_l(n) = \alpha\pi_l(n)$, $N_0 = N/K$

$\pi(n)$ — ПСП $\{\pm 1\}$ и является СК легального пользователя.

В простейшем случае K=2 и тогда любой пользователь может оценить значение функционала $\Lambda = \sum_{n=1}^{N_0} s(n)s(n+N_0)$, сравнить с порогом λ и поскольку принято, что стегасообщение не подвергается преобразованию нелегальным пользователем, если в нем присутствует ВЗ, т.е. $s'(n) = s(n)$, то

$$\Lambda = \Lambda_1 = \sum_{n=1}^{N_0}(c(n) + w(n))(c(n+N_0) + w(n)) =$$

$$= \sum_{n=1}^{N} c(n)c(n+N_0) + \sum_{n=1}^{N_0} w(n)(c(n) + c(n+N_0)) + \alpha^2 N$$

и в случае отсутствия ВЗ

$$\Lambda = \Lambda_0 = \sum_{n=1}^{N_0} c(n)c(n+N_0)$$

Поскольку все элементы стегосообщения в соответствие с принятой моделью являются гауссовыми, то и функционалы детекторов Λ_0 и Λ_1 также будут гауссовыми величинами, причем $E(\Lambda_0) = 0$, $E(\Lambda_1) = \alpha^2 N$, $Var\Lambda_0 = NE(c^2(n))E(c^2(n+N_0)) = N\sigma_c^4$, $n = 1,2\ldots, 2N_o$. Если $c(n)$ и $c(n+N_o)$ не коррелированны, то $Var\Lambda_1 = N(\sigma_c^4 + 2\alpha^2\sigma_c^2)$ и выражения для вероятностей ошибок (17), (18) для рассматриваемого сценария можно представить в виде

$$P_m = 1 - Q\left(\frac{\lambda - \alpha^2 N}{\sqrt{N(\sigma_c^4 + 2\alpha^2 \sigma_c^2}}\right), \tag{27}$$

$$P_{fa} = Q\left(\frac{\lambda}{\sqrt{N\sigma_c^4}}\right) \tag{28}$$

или с использованием параметра искажения $\eta_w = \frac{Var(c(n))}{Var(w(n))} = \frac{\sigma_c^2}{\alpha^2}$

$$P_m = 1 - Q((\lambda' - 1)\sqrt{\frac{N}{\eta_w^2 + 2\eta_w}}) \approx 1 - Q((\lambda' - 1)\sqrt{\frac{N}{\eta_w^2}}) \tag{29}$$

$$P_{fa} = Q(\lambda'\sqrt{\frac{N}{\eta_w^2}}) \tag{30}$$

где $\lambda' = \frac{\lambda_0}{\alpha^2 N}$

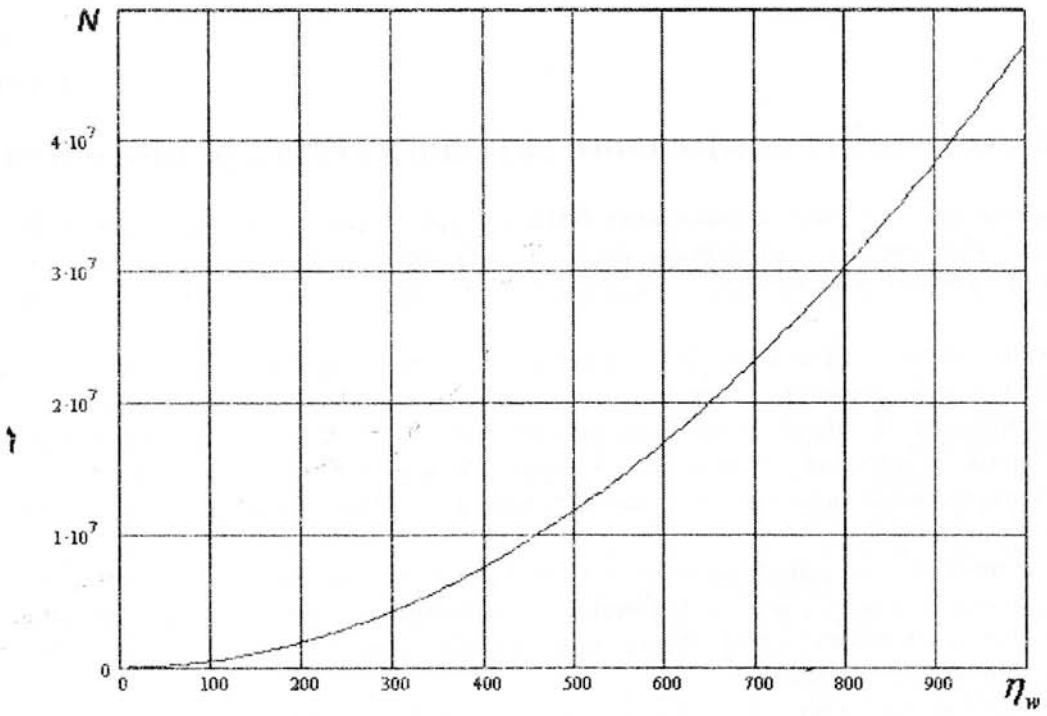

Рис.2. Зависимость числа бит периодических ВЗ N от величины η_W для случаев $\eta = 1{,}5$ при использовании нелегальным пользователем неинформированного детектора в условиях атаки аддитивным шумом при отсутствие ВЗ и выполнении соотношения $P_m = P_{fa} = 10^{-3}$

Из анализа (30) и (29) и полученных численных результатов очевидно значительное ухудшение эффективности системы. Действительно, при увеличении параметра искажений η_w, например, в m раз необходимо для сохранения вероятностей ошибок секретной

системы на заданном уровне увеличить N в m раз, а для рассматриваемого сценария полусекретной системы для фиксированных значений вероятностей ошибок необходимо увеличить длину ВЗ N в m^2 раз. Данный эффект аналогичен квадратичной компенсации некогерентного приемника широкополосных систем [4]. С другой стороны, длина ВЗ ограничивается надежностью восприятия. Таким образом, если предыдущий сценарий полусекретной системы ограничивался соотношением $\eta_a \approx \eta_w$, то в данном случае необходимо решать компромисс между надежностью восприятия (длиной ВЗ) и вероятностями ошибок детектирования в более жестких условиях.

Список литературы

1. Goldberg E.I. Negative Thinking by Incremental Problem Solving: Application to Unite Covering // International Conference on Computer Aided Design. —1997.—P.91—99.
2. Маракова И.И. Секретные системы с цифровими водяными знаками в условиях атаки в виде ади-тивного шума и линейной фильтрации// Захист інформації. — Киев. — 2003. — №2. —С.41—46
3. Маракова И.И., Мараков Д.А., Оценка эффективности систем со скрытыми цифровыми метками// Труды Одесск. нац. политех. Ун-та. — 2002. — вып.2, С.110—115
4. Миддлтон Д. Введение в статистическую теорию связи. Т.1, 2. —М.: Сов. радио, 1961.—728с.

Поступила 27.04.2004
После доработки 19.05.2004

УДК 655.77.13

І.О.Козлюк

ОЦІНКА ТЕХНІКО-ТЕХНОЛОГІЧНОЇ БЕЗПЕКИ В ТРАНСПОРТНІЙ СИСТЕМІ

Ключовою складовою економічної безпеки транспорту в контексті довгострокового розвитку та забезпечення сприятливих перспектив участі країни в транспортної системі та міжнародної конкурентноздатності національного виробництва є техніко-технологічна безпека.

Техніко-технологічна безпека транспортної системи України полягає у впровадженні новітніх технологій, досягненні технічного прогресу, збереженні такого рівня вітчизняного науково-технічного й виробничого потенціалу, який у разі погіршення внутрішніх і зовнішніх умов забезпечив би виживання національної економіки в галузі транспорту за рахунок використання власних інтелектуальних і технологічних ресурсів, збереження державної незалежності.

Технічний прогрес, який включає в себе, крім нових методів виробництва, ще й нові форми управління та організації виробництва, є найважливішим чинником, що впливає на підвищення продуктивності праці. Технології є одним з основних чинників, які зумовлюють здатність економіки до зростання.

Функціональний критерій техніко-технологічної безпеки підприємства ($ФК$) [1-3] розраховується за формулою:

$$ФК = \frac{З_{відв}}{В_{ркз} + З_{завд}} \rightarrow мах$$

де $З_{відв}$ - сумарний відвернений збиток від реалізації комплексу техніко-технологічних заходів;