

**Науменко Данила Олегович** – e-mail: dante603@gmail.com; 355040, г. Ставрополь, ул. Семашко, 8, кв. 23; тел.: 89197362888; кафедра информационной безопасности автоматизированных систем; аспирант.

**Калмыков Максим Игоревич** – e-mail: kmi762@yandex.ru; 355040, г. Ставрополь, пр. Кулакова, 33, кв. 56; тел.: 88652956546; кафедра информационной безопасности автоматизированных систем; аспирант.

**Kalmykov Igor Anatolyevich** – Institute of Information Technologies and Telecommunications, North-Caucasus Federal University, Stavropol; e-mail: kia762@yandex.ru; 92, Shpakovskaya street, k.1, kv. 28, Stavropol, 355000, Russia; phone: +78652731380, +79034163533; the department of information security of automated systems; dr. of eng. sc.; professor.

**Velts Oksana Vladimirovna** – e-mail: velts-yatsenco@yandex.ru; 33, Chehova street, kv. 66, Stavropol, 355000, Russia; phone: +78652944241; the department of information science; senior lecturer.

**Naumenko Daniil Olegovich** – e-mail: dante603@gmail.com; 8, Semashko street, kv. 23, Stavropol, 355000, Russia; phone: +79197362888; the department of information security of automated systems; postgraduate student.

**Kalmykov Maksim Igorevich** – e-mail: kmi762@yandex.ru; 33, pr. Kulakova, kv. 44, Stavropol, 355040, Russia; phone: +79064710242; the department of information security of automated systems; postgraduate student.

УДК 621.39

**С.В. Котенко**

### **ИДЕНТИФИКАЦИОННЫЙ АНАЛИЗ ПРОЦЕССОВ ТЕЛЕКОММУНИКАЦИИ НЕПРЕРЫВНЫХ СООБЩЕНИЙ В ЦИФРОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ**

*На фоне значительных достижений в части идентификации пользователей информационно-телекоммуникационных систем в задачах обработки, защиты и передачи информации практически обходится вниманием идентификация (аутентификация) информационно-телекоммуникационных процессов. Следствием этого является отсутствие самого понятия «идентификационный анализ» применительно к информационно-телекоммуникационным системам, не смотря на апробированные результаты продуктивного применения этого понятия к производственным, маркетинговым и педагогическим системам. Критичность сложившейся ситуации заключается в выявленных в последнее время закономерностях, состоящих в значительном и в ряде случаев определяющем влиянии пользовательского уровня на эффективность информационно-телекоммуникационных процессов. Приводится решение задачи теоретического обоснования методики идентификационного анализа процессов телекоммуникации непрерывных сообщений в цифровых информационных системах с позиций подходов и методов теории виртуализации. По результатам полученного решения синтезирована модель идентификационного анализа, включающая канал виртуальной оценки, что обеспечивает потенциально защищенную идентификацию. Отличительную особенность предложенной методики составляет применение в качестве идентификационных признаков адаптивно изменяющихся параметров цифрового представления непрерывных сообщений в цифровых информационных системах.*

*Идентификация; аутентификация; виртуализация; идентификационный анализ; информационный поток.*

S.V. Kotenko

## IDENTIFICATION ANALYSIS OF PROCESSES TELECOMMUNICATIONS OF CONTINUOUS REPORTS IN DIGITAL INFORMATION SYSTEMS

*On the background of the significant achievements in terms of user identification information and telecommunication systems in the tasks of processing, protection and transmission of information on almost overlook identification ( authentication) information and telecommunication processes. The consequence of this is the lack of the concept of «identification analysis» in relation to information and telecommunication systems , despite the proven results of productive application of this concept to production, marketing and educational systems. Criticality of the situation is revealed recently the patterns consisting of a measurable and in some cases, which determines the impact on the efficiency of user-level information and telecommunications processes. The article provides a solution to the problem of theoretical justification identification process analysis techniques telecommunications continuous messages in digital information systems from the standpoint of the approaches and methods of the theory of virtualization. According to the results of the solution synthesized model identification analysis, including virtual channel estimates that potentially provides a secure identification. Distinctive feature of the proposed method is used as indicia adaptively changing the parameters of the digital representation of continuous messages in digital information systems.*

*Authentication; authentication; virtualization; identification analysis; dataflow.*

Идентификационный анализ информационно-телекоммуникационных систем является комплексным понятием, включающим идентификацию и аутентификацию пользовательского уровня и информационно-телекоммуникационных процессов. Анализ ситуации, сложившейся в данном научном направлении показывает отсутствие решений проблемы комплексной идентификации (аутентификации) пользователей и информационных процессов телекоммуникационных систем. При этом на фоне значительных достижений в части идентификации пользователей в задачах обработки, защиты и передачи информации практически обходится вниманием идентификация (аутентификация) информационно-телекоммуникационных процессов. Следствием этого является отсутствие самого понятия «идентификационный анализ» применительно к информационно-телекоммуникационным системам (при достаточно широком и продуктивном применении этого понятия к производственным, маркетинговым и педагогическим системам). Критичность сложившейся ситуации заключается в выявленных в последнее время закономерностях, состоящих в значительном (в ряде случаев определяющем) влиянии пользовательского уровня на эффективность информационно-телекоммуникационных процессов. Таким образом, исследования в области идентификационного анализа процессов телекоммуникации являются актуальными и имеют значительное научное и практическое значение.

Целью исследований является разработка методики идентификационного анализа процессов телекоммуникации непрерывных сообщений в цифровых информационных системах на основе подходов и методов теории виртуализации.

Значительный научный и практический опыт исследований процессов телекоммуникации [1, 2, 3] показывает предпочтительность представления непрерывных сообщений в виде стационарного гауссовского марковского случайного процесса, описываемого априорным дифференциальным уравнением вида:

$$\frac{d\mathbf{S}(t)}{dt} = \mathbf{A}(t)\mathbf{S}(t) + \mathbf{\Gamma}(t)\mathbf{N}_S(t), \quad (1)$$

где  $\mathbf{S}(t)$  и  $\mathbf{N}_S(t)$  – матрицы столбцы размером  $r$ ;  $\mathbf{A}(t)$  и  $\mathbf{\Gamma}(t)$  – матрицы размером  $r \times r$ .

Вектор  $\mathbf{N}_S(t)$  представляет собой формирующий белый стационарный шум с независимыми компонентами:

$$M[\mathbf{N}_S(t)] = 0, M[\mathbf{N}_S(t)\mathbf{N}_S^T(t + \tau)] = 0,5 \mathbf{B}_S \delta(\tau),$$

где  $\delta(\tau)$  – дельта-функция;  $\mathbf{B}_S$  – диагональная матрица спектральных плотностей формирующего шума.

В процессе цифровой обработки аналоговых сообщений общепринято [3] выделять три этапа: дискретизация, квантование и кодирование. Дискретизация исходного процесса осуществляется путём точечного выбора

$$\mathbf{S}(i) = \mathbf{S}(t_i) = \int_{-\infty}^{+\infty} \mathbf{S}(t) \delta(iT - t) dt.$$

В результате дискретизации образуется векторная марковская последовательность  $\mathbf{S}(t_i) = \mathbf{S}(i)$ , определяемая рекуррентным уравнением вида

$$\mathbf{S}(i) = \Phi_{i,i-1} \mathbf{S}(i) + \mathbf{G}_i \mathbf{N}(i), \quad (2)$$

где  $\mathbf{S}(i)$  и  $\mathbf{N}(i)$  – матрицы столбцы;  $\Phi_{i,i-1}$  и  $\mathbf{G}_i$  – квадратные матрицы  $r \times r$ .

Элементы матрицы  $\Phi_{i,i-1}$  определяются как

$$\text{fnl}(t_i, t_{i-1}) = -\text{Anl}(t_i, t_{i-1}) / d_1,$$

где  $d_1$  – определитель корреляционной матрицы вектора  $\mathbf{S}_{i-1}$ ;  $\text{Anl}(t_i, t_{i-1})$  – алгебраическое дополнение корреляционной матрицы вектора  $[\mathbf{S}_n(t_i), \mathbf{S}_1(t_{i-1}), \dots, \mathbf{S}_1(t_{i-1}), \dots, \mathbf{S}_r(t_{i-1})]^T$ , соответствующее компонентам  $\mathbf{S}_n(t_i)$  и  $\mathbf{S}_1(t_{i-1})$ .

Вектор-столбец  $\mathbf{G}_i \mathbf{N}(i)$  характеризуется нулевой матрицей математических ожиданий и диагональной дисперсионной матрицей

$$\mathbf{D}_N(i) = \mathbf{D}_S(i) - \Phi_{i,i-1} \mathbf{D}_S(i-1) \Phi_{i,i-1}^T.$$

В результате квантования образуется векторная дискретная последовательность

$$\Psi[\mathbf{S}(i)] = \Psi_{(i)}^{(n)}, \quad \mathbf{S}(i) \in \Theta^{(n)}, \quad (3)$$

где  $\Theta^{(n)}$  – область квантования;  $n$  – номер области квантования.

Учитывая детерминированность процедуры квантования [3], считается, что компоненты вектора сообщения  $\mathbf{S}_k(t_i)$  квантуются отдельно друг от друга. В результате такого квантования образуются векторные величины  $\Psi_i = \Psi[\mathbf{S}_i] = [\Psi_1(t_i), \Psi_2(t_i) \dots \Psi_r(t_i)]^T$ , представляющие собой векторы-столбцы. Потери, вызванные квантованием, принято представлять в виде шума квантования и обозначать как

$$\mathbf{W}(i) = \mathbf{S}(i) - \Psi(i). \quad (4)$$

В процессе кодирования векторная величина  $\Psi_i$  преобразуется в соответствующее ей цифровое сообщение  $\mathbf{X}_i$ , вид которого определяется используемым кодом. Цифровое сообщение может быть векторным, если разделяется на компоненты, представляющие собой кодовые комбинации, которые соответствуют составляющим вектора сообщений, или скалярным, если представляет собой кодовую комбинацию, соответствующую номеру области квантования, в которую попадает вектор квантуемого сообщения.

Если на процедуру кодирования не накладывается никаких ограничений, вектор  $\Psi_i$  и вектор  $X_i$  принято отождествлять, когда в этом появляется необходимость. Исходя из этого, в случаях, когда в качестве исходного рассматривается процесс, заданный выражением (2), шум квантования можно рассматривать как шум цифрового представления

Решение задачи идентификационного анализа для рассматриваемого случая может осуществляться по двум основным направлениям:

1) использование в качестве идентификационного признака, коррелированного с сообщением шума его цифрового представления  $W(i)$ ;

2) использование в качестве идентификационного признака кодовой последовательности  $N_K(i)$ , формируемой из шума цифрового представления сообщения по закону идентификационного ключа  $K$ .

При этом необходимо подчеркнуть, что предложенный подход не накладывает ограничений на число вариантов возможного использования шума цифрового представления (шума квантования) при решении задач идентификационного анализа аналоговых сообщений в цифровых системах связи. Однако с достаточной степенью уверенности можно предположить, что всем этим вариантам будут присущи некоторые общие черты, связанные с особенностями самой процедуры квантования. Исходя из этого, можно считать, что общие черты будут присущи и решениям задач, которые используют данные варианты. Это даёт основание считать продуктивным путь анализа возможностей разрабатываемой методики, состоящий в выборе некоторого исходного варианта, его решение и последующее обобщение результатов этого решения на другие варианты.

Исходным выберем вариант использования в качестве идентификационного признака коррелированного с сообщением шума его цифрового представления. При этом введем условие виртуализации.

**Условие 1.** Сообщения в цифровой системе телекоммуникации формируются как результат аддитивной композиции цифрового представления непрерывного сообщения пользователя и шума цифрового представления предыдущего сообщения пользователя.

Соответствующее условию 1 виртуальное сообщение может быть представлено в виде:

$$\tilde{Z}(i) = \Psi(i) + W(i-j) \quad (5)$$

где  $\tilde{Z}(i)$  – виртуальное сообщение;  $\Psi(i)$  – цифровое представление исходного непрерывного сообщения;  $W(i-j)$  – шум цифрового представления предыдущего исходного непрерывного сообщения

Будем считать, что при передаче виртуальное сообщение подвергается искажениям, которые можно трактовать как воздействие аддитивного шума наблюдения  $V(i)$ . Этот шум считается гауссовским, не зависящим от сообщения, с независимыми компонентами и значениями. Он задаётся нулевой матрицей математических ожиданий и диагональной дисперсионной матрицей  $D_V(i)$ . Таким образом, модель наблюдения  $Y(i)$  на выходе канала связи может быть представлена в виде

$$\begin{aligned} Y(i) &= H_i \tilde{Z}(i) + V(i) = H_i \Psi(i) + H_i W(i-j) + V(i) = \\ &= H_i S(i-j) + (H_i \Psi(i) - H_i \Psi(i-j) + V(i)) \end{aligned} \quad (6)$$

Обозначим

$$H_i \Psi(i) - H_i \Psi(i-j) + V(i) = \lambda(i). \quad (7)$$

Тогда (6) преобразуется к виду

$$\mathbf{Y}(i) = \mathbf{H}_i \mathbf{S}(i-j) + \boldsymbol{\lambda}(i). \quad (8)$$

Принимая во внимание, что наблюдение (8) применительно к условию 1 формируется из виртуального сообщения, обозначим его как виртуальное представление наблюдения. При этом необходимо учитывать, что условие 1 не накладывает ограничений на формирование действительного представления наблюдения из цифрового представления сообщения

$$\mathbf{Y}(i) = \mathbf{H}_i \boldsymbol{\Psi}(i) + \mathbf{V}(i). \quad (9)$$

Таким образом, предложенный подход позволяет формировать два варианта представления наблюдения, что открывает возможность идентификационного анализа в реальном масштабе времени. Основная задача идентификационного анализа в этом случае сводится к задаче формирования оценок (задаче фильтрации) сообщений из действительной и виртуальной форм наблюдения и количественного сравнения  $i$ -й и  $(i-j)$ -й оценок. При этом из наблюдения  $\mathbf{Y}(i)$  формируются две оценки: 1) оценка  $\mathbf{S}^*(i)$  из действительной формы наблюдения; 2) оценка  $\mathbf{S}^*(i-j)$  из виртуальной формы наблюдения. Эти оценки определяются как действительная и виртуальная. Причем виртуальная оценка однозначно соответствует действительной оценке, сформированной на  $(i-j)$ -м такте. Сравнение этих оценок составляет основу идентификационного анализа.

Анализ выражений (8) показывает, что задача формирования оценки по действительной форме представления наблюдения сводится к известной задаче нелинейной фильтрации аналоговых сообщений в системах с импульсно-кодовой модуляцией [3]. Задача формирования оценки по виртуальной форме представления наблюдения на основании (8) сводится к достаточно своеобразной задаче линейной интерполяционной фильтрации с шумом наблюдения, нелинейно зависимым от сообщения. Решение этой задачи в прямой постановке не представляется возможным. Далее представлен оригинальный подход к ее решению для скалярного представления.

Ставится задача синтеза алгоритма оценки сообщения (2) по наблюдению (8). Оценка оптимальная по критерию минимума среднего квадрата ошибки (СКО) может быть определена из исходного выражения вида:

$$\tilde{s}_i^* = \int_{-\infty}^{+\infty} s_i P[s_i / \tilde{y}_1^{i+1}] ds_i. \quad (10)$$

Здесь выражение для апостериорной плотности вероятностей может быть представлено как:

$$P[s_i / \tilde{y}_1^{i+1}] = \frac{1}{P[\tilde{y}_1^{i+1}]} \int_{-\infty}^{+\infty} P[s_i, s_{i-1}, \tilde{y}_1^{i+1}] ds_{i-1}, \quad (11)$$

где

$$\begin{aligned} P[s_i, s_{i-1}, \tilde{y}_1^{i+1}] &= P[s_i, s_{i-1}, \tilde{y}_{i+1}, \tilde{y}_1^i] = \\ &= P[\tilde{y}_1^i] P[s_{i-1} / \tilde{y}_1^i] P[s_i / s_{i-1} \tilde{y}_1^i] P[\tilde{y}_{i+1} / s_i s_{i-1} \tilde{y}_1^i] \end{aligned} \quad (12)$$

Учитывая марковость процесса  $s_i$  можно записать:

$$P[s_i / s_{i-1} \tilde{y}_1^i] = P[s_i / s_{i-1}]. \quad (13)$$

Условную вероятность  $P[\tilde{y}_{i+1} / s_i, s_{i-1}, \tilde{y}_1^i]$  можно представить как:

$$\begin{aligned}
P[\tilde{y}_{i+1} / s_i, s_{i-1}, \tilde{y}_1^i] &= \frac{P[\tilde{y}_{i+1}, s_i, s_{i-1}, \tilde{y}_1^i]}{P[s_i, s_{i-1}, \tilde{y}_1^i]} = \\
&= P[\tilde{y}_{i+1} / s_{i-1}, \tilde{y}_1^i] \frac{P[s_i / s_{i-1}, \tilde{y}_1^{i+1}]}{P[s_i / s_{i-1}, \tilde{y}_1^i]}
\end{aligned} \tag{14}$$

Откуда получаем:

$$\begin{aligned}
P[s_i / \tilde{y}_1^{i+1}] &= \frac{P[\tilde{y}_1^i]}{P[\tilde{y}_1^{i+1}]} \times \\
&\times \int_{-\infty}^{+\infty} P[\tilde{y}_{i+1} / s_{i-1}, \tilde{y}_1^i] \frac{P[s_i / s_{i-1}, \tilde{y}_1^{i+1}]}{P[s_i / s_{i-1}, \tilde{y}_1^i]} P[s_i / s_{i-1}] P[s_{i-1} / \tilde{y}_1^i] ds_{i-1}.
\end{aligned} \tag{15}$$

Полученное выражение задаёт рекуррентный алгоритм определения апостериорной вероятности. С учётом (15) выражение для оценки  $\tilde{S}_i^*$  может быть представлено в виде:

$$\begin{aligned}
\tilde{S}_i^* &= \frac{P[\tilde{y}_1^i]}{P[\tilde{y}_1^{i+1}]} \times \\
&\times \int_{-\infty}^{+\infty} \int P[\tilde{y}_{i+1} / s_{i-1}, \tilde{y}_1^i] \frac{P[s_i / s_{i-1}, \tilde{y}_1^{i+1}]}{P[s_i / s_{i-1}, \tilde{y}_1^i]} s_i P[s_i / s_{i-1}] P[s_{i-1} / \tilde{y}_1^i] ds_{i-1} ds_i.
\end{aligned} \tag{16}$$

Проведём анализ физического смысла отношения апостериорных вероятностей, для чего возьмём логарифм от этого отношения:

$$\begin{aligned}
\ln \frac{P[s_i / s_{i-1}, \tilde{y}_1^{i+1}]}{P[s_i / s_{i-1}, \tilde{y}_1^i]} &= \ln \frac{P[s_i] P[s_i / s_{i-1}, \tilde{y}_1^{i+1}]}{P[s_i] P[s_i / s_{i-1}, \tilde{y}_1^i]} = \\
&= \ln \frac{P[s_i / s_{i-1}, \tilde{y}_1^{i+1}]}{P[s_i]} - \ln \frac{P[s_i / s_{i-1}, \tilde{y}_1^i]}{P[s_i]} = \\
&= J[s_i; s_{i-1}, \tilde{y}_1^{i+1}] - J[s_i; s_{i-1}, \tilde{y}_1^i].
\end{aligned} \tag{17}$$

где

$$J[s_i; s_{i-1}, \tilde{y}_1^{i+1}] = \ln \frac{P[s_i / s_{i-1}, \tilde{y}_1^{i+1}]}{P[s_i]}, \tag{18}$$

$$J[s_i; s_{i-1}, \tilde{y}_1^i] = \ln \frac{P[s_i / s_{i-1}, \tilde{y}_1^i]}{P[s_i]}. \tag{19}$$

С позиций теории информации выражение (18) определяет количество информации о сообщении  $S_i$ , содержащееся в  $S_{i-1}$  и  $\tilde{Y}_{i+1}$ , а выражение (19) – количество информации о  $S_i$ , содержащееся в  $S_{i-1}$  и  $\tilde{Y}_1^i$ .

Это дает основание считать, что отношение апостериорных вероятностей в (17) характеризует изменение количества информации о сообщении  $S_i$  после поступления наблюдения  $\tilde{Y}_{i+1}$  при известных  $S_{i-1}$  и  $\tilde{Y}_1^i$ . Нетрудно заметить, что с позиций реальных задач связи анализируемое отношение является в достаточной степени абстрактным, так как сообщение  $S_{i-1}$  никогда не может быть точно известно на приеме. Можно говорить только об оценке  $S_{i-1}^*$  этого сообщения, полученного с той или иной точностью. С этих позиций докажем допустимость равенства:

$$\frac{P[S_i / S_{i-1}, \tilde{Y}_1^{i+1}]}{P[S_i / S_{i-1}, \tilde{Y}_1^i]} = \frac{P[S_i / S_{i-1}^*, \tilde{Y}_1^{i+1}]}{P[S_i / S_{i-1}^*, \tilde{Y}_1^i]}. \quad (20)$$

Точность оценки  $S_{i-1}^*$  может характеризоваться, как потеря некоторого количества информации  $J_{\Pi}(e_{i-1})$  об  $S_{i-1}$  в результате неточного воспроизведения  $S_{i-1}$  на приеме с ошибкой  $e_{i-1} = S_{i-1} - \tilde{S}_{i-1}^*$ . Таким образом, исходя из (17) можно записать:

$$\begin{aligned} \ln \frac{P[S_i / S_{i-1}, \tilde{Y}_1^{i+1}]}{P[S_i / S_{i-1}, \tilde{Y}_1^i]} &= J[S_i; S_{i-1}, \tilde{Y}_1^{i+1}] - J[S_i; S_{i-1}, \tilde{Y}_1^i] = \\ &= J[S_i; \tilde{S}_{i-1}^*, \tilde{Y}_1^{i+1}] - J_{\Pi}(e_{i-1}) - J[S_i; \tilde{S}_{i-1}^*, \tilde{Y}_1^i] + J_{\Pi}(e_{i-1}) = \\ &= \ln \frac{P[S_i / \tilde{S}_{i-1}^*, \tilde{Y}_1^{i+1}]}{P[S_i / \tilde{S}_{i-1}^*, \tilde{Y}_1^i]} \end{aligned} \quad (21)$$

Соотношение (21) доказывает допустимость равенства (20).

Исходя из тех же соображений, разложим условную плотность вероятности

$P[S_i / S_{i-1}]$  по  $S_{i-1}$  в ряд в точке  $S_{i-1} = \tilde{S}_{i-1}^*$ :

$$\begin{aligned} P[S_i / S_{i-1}] &= P[S_i / \tilde{S}_{i-1}^*] + P'[S_i / \tilde{S}_{i-1}^*](S_{i-1} - \tilde{S}_{i-1}^*) + \\ &+ \frac{1}{2} P''[S_i / \tilde{S}_{i-1}^*](S_{i-1} - \tilde{S}_{i-1}^*)^2 + \dots \end{aligned} \quad (22)$$

Подставив (22) в (16), по известной методике [3] получим

$$\tilde{S}_i^* = \frac{P[\tilde{Y}_1^i]}{P[\tilde{Y}_1^{i+1}]} \int_{-\infty}^{+\infty} P[\tilde{Y}_{i+1} / \tilde{S}_{i-1}^* \tilde{Y}_1^i] \frac{P[S_i / \tilde{S}_{i-1}^* \tilde{Y}_1^{i+1}]}{P[S_i / \tilde{S}_{i-1}^* \tilde{Y}_1^i]} S_i P[S_i / \tilde{S}_{i-1}^*] dS_i \quad (23)$$

Далее ограничимся высокой точностью оценивания, что позволяет считать вектор  $(S_i, \tilde{S}_{i-1}^*)^T$  гауссовским, а плотность вероятностей  $P[S_i / \tilde{S}_{i-1}^*]$  – нормальной. С учётом этого  $P[S_i / \tilde{S}_{i-1}^*]$  может быть представлена как [2]:

$$P[S_i / \tilde{S}_{i-1}^*] = e^{-(S_i - \Phi_{\tilde{S}_{i-1}^*})^2 / 2D_i}, \quad (24)$$

где  $D_i$  – апостериорная дисперсия на  $i$ -м шаге.

Отношение апостериорных вероятностей в (23), как уже отмечалось, характеризует изменение количества информации о сообщении после поступления  $(i+1)$ -го наблюдения  $Y_{i+1}$  при уже известных  $\tilde{S}_{i-1}^*$  и  $\tilde{Y}_1^i$ . Это даёт основание допустить, что

данное отношение представляет собой некоторую функцию, изменяющуюся прямо пропорционально количеству **новой** информации о сообщении, содержащейся в  $\tilde{y}_{i+1}$ :

$$F(\tilde{y}_{i+1}; \tilde{s}_{i-1}^*, \tilde{y}_1^i) \triangleq \frac{P[s_i / \tilde{s}_{i-1}^* \tilde{y}_1^{i+1}]}{P[s_i / \tilde{s}_{i-1}^* \tilde{y}_1^i]}, \quad (25)$$

где знаком  $\triangleq$  будем обозначать равенство по определению.

Правомочность такого допущения, конечно, требует проверки, однако его логичность вполне обоснована положительными результатами аналогичных допущений, принятых при решении похожих задач (синтез алгоритмов Калмана).

С учётом (25) выражение для оценки принимает вид:

$$\tilde{s}_i^* = \frac{P[\tilde{y}_1^i]}{P[\tilde{y}_1^{i+1}]} \cdot F(\tilde{y}_1^{i+1}; \tilde{s}_{i-1}^*, \tilde{y}_1^i) \int_{-\infty}^{+\infty} P[\tilde{y}_{i+1} / \tilde{s}_{i-1}^* \tilde{y}_1^i] s_i P[s_i / \tilde{s}_{i-1}^*] ds_i. \quad (26)$$

Можно доказать, что

$$P[\tilde{y}_{i+1} / \tilde{s}_{i-1}^* \tilde{y}_1^i] = P[\tilde{y}_{i+1} / \tilde{y}_1^i].$$

Таким образом, можно записать:

$$\tilde{s}_i^* = \frac{P[\tilde{y}_1^i]}{P[\tilde{y}_1^{i+1}]} \cdot F(\tilde{y}_{i+1}; \tilde{s}_{i-1}^*, \tilde{y}_1^i) \int_{-\infty}^{+\infty} P[\tilde{y}_{i+1} / \tilde{y}_1^i] s_i P[s_i / \tilde{s}_{i-1}^*] ds_i. \quad (27)$$

Запишем интеграл в правой части (27) в виде:

$$\begin{aligned} & \int_{-\infty}^{+\infty} P[\tilde{y}_{i+1} / \tilde{y}_1^i] s_i P[s_i / \tilde{s}_{i-1}^*] ds_i = \\ & = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} P[\tilde{y}_{i+1} \tilde{\lambda}_{i+1} / \tilde{y}_1^i] s_i P[s_i / \tilde{s}_{i-1}^*] d\tilde{\lambda}_{i+1} ds_i = \\ & = P[\tilde{y}_{i+1}] \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} P[\tilde{\lambda}_{i+1} / \tilde{y}_1^{i+1}] s_i P[s_i / \tilde{s}_{i-1}^*] d\tilde{\lambda}_{i+1} ds_i \end{aligned} \quad (28)$$

Согласно постановке задачи:

$$\tilde{y}_{i+1} = \mathbf{H}_{i+1} s_i + \tilde{\lambda}_{i+1}. \quad (29)$$

Отсюда

$$s_i = \mathbf{H}_{i+1}^{-1} \tilde{y}_{i+1} - \mathbf{H}_{i+1}^{-1} \tilde{\lambda}_{i+1}. \quad (30)$$

Подставив (28) в (27) с учётом (30), получим

$$\begin{aligned} \tilde{s}_i^* &= F(\tilde{y}_{i+1}, \tilde{s}_{i-1}^*) \cdot \frac{P[\tilde{y}_1^i]}{P[\tilde{y}_1^{i+1}]} P[\tilde{y}_{i+1}] \mathbf{H}_{i+1}^{-1} \times \\ & \times \left\{ \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \tilde{y}_{i+1} P[\tilde{\lambda}_{i+1} / \tilde{y}_1^{i+1}] P[s_i / \tilde{s}_{i-1}^*] d\tilde{\lambda}_{i+1} ds_i - \right. \\ & \left. - \int_{-\infty}^{+\infty} P[s_i / \tilde{s}_{i-1}^*] \int_{-\infty}^{+\infty} \tilde{\lambda}_i P[\tilde{\lambda}_{i+1} / \tilde{y}_1^{i+1}] d\tilde{\lambda}_{i+1} ds_i \right\}. \end{aligned} \quad (31)$$

В полученном выражении



$$\frac{P[\tilde{y}_1^i]}{P[\tilde{y}_1^{i+1}]} \cdot P[\tilde{y}_{i+1}] = \frac{P[\tilde{y}_{i+1}]}{P[\tilde{y}_{i+1}/\tilde{y}_1^i]}, \quad \tilde{\lambda}_{i+1}^* = \int_{-\infty}^{+\infty} \tilde{\lambda}_{i+1} P[\tilde{\lambda}_{i+1}/\tilde{y}_1^{i+1}] d\tilde{\lambda}_{i+1}.$$

Согласно постановке задачи:

$$\tilde{\lambda}_{i+1} = \mathbf{H}_{i+1} (\Psi(i+1) - \Psi(i)) + v(i) = \mathbf{H}_{i+1} \Delta\Psi(i+1, i) + v(i).$$

Отсюда можно допустить возможность представления:

$$\tilde{\lambda}_{i+1}^* = \mathbf{K}_{i+1, i}' \mathbf{H}_i \Delta\Psi^*(i+1, i), \quad (32)$$

где  $\mathbf{K}_{i+1, i}'$  – можно трактовать как некоторый переменный коэффициент усиления, характеризующий воздействие помех в канале связи.

Произведя интегрирование в (31) с учётом (32), получим

$$\tilde{s}_i^* = F(\tilde{y}_{i+1}, \tilde{s}_{i-1}^*) \mathbf{K}_{i, i+1} (\tilde{y}_{i+1} - \mathbf{H}_{i+1} \mathbf{K}_{i+1, i}' \Delta\Psi^*(i+1, i)), \quad (33)$$

где

$$\mathbf{K}_{i, i+1} = \frac{P[\tilde{y}_{i+1}]}{P[\tilde{y}_{i+1}/\tilde{y}_1^i]} \sqrt{2\pi} D_i^{1/2} \mathbf{H}_{i+1}^{-1}.$$

Модель полученного решения, то есть модель идентификационного анализа процессов телекоммуникации непрерывных сообщений в цифровых информационных системах с позиций виртуализации сообщений и оценок, приведена на рис. 1. При отображении модели учитывалась физическая однозначность виртуального и реального наблюдений  $y_i = \tilde{y}_i$ .

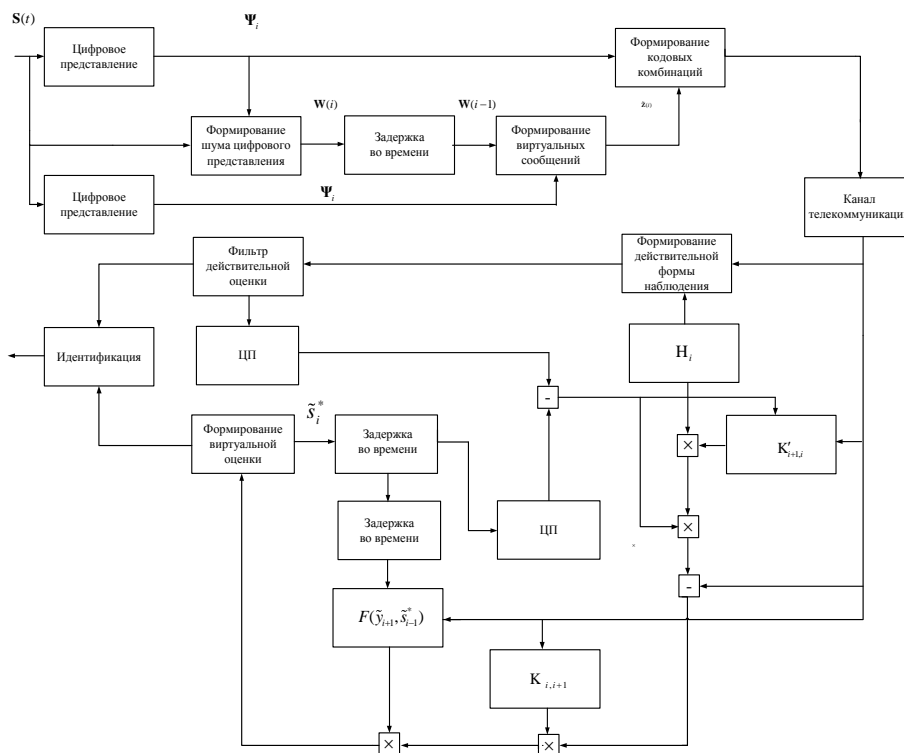


Рис. 1. Модель идентификационного анализа процессов телекоммуникации непрерывных сообщений в цифровых информационных системах

**Выводы.** Принципиальной особенностью полученной модели является включение канала виртуальной оценки, обеспечивающее применение в качестве идентификационных признаков адаптивно изменяющихся параметров цифрового представления. Следует подчеркнуть, что полученное решение не является однозначно оптимальным. Это объясняется целью, которая ставилась при его синтезе – определить методику решения задач идентификационного анализа процессов телекоммуникации непрерывных сообщений в цифровых информационных системах. Более того, учитывая новизну решаемой задачи, ряд допущений принятых при выводе алгоритма виртуальной оценки требуют проверки и в свою очередь определяют направления дальнейших исследований. Однако это не влияет на понимание физики процесса включения канала виртуальной оценки в синтезированной модели в целях обеспечения защищенной идентификации.

#### БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Котенко В.В., Румянцев К.Е.* Теория информации и защита телекоммуникаций: Монография. – Ростов-на-Дону: Изд-во ЮФУ, 2009. – 369 с.
2. *Котенко В.В.* Теоретическое обоснование виртуальных оценок в защищенных телекоммуникациях // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 177-183.
3. *Котенко С.В., Румянцев К.Е.* Компьютерное моделирование технологии аурикулодиагностической идентификации // Труды научно-технической конференции с международным участием «Компьютерное моделирование в наукоемких технологиях» (КМНТ-2010). Часть 2. – Харьков Изд-во ХНУ, 2010. – С. 128-131.
4. *Румянцев К.Е., Котенко С.В.* Эффективность виртуальной аурикулодиагностической идентификации // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 2. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 170-175
5. *Kotenko V., Rumjantsev K., Kotenko S.* New Approach to Evaluate the Effectiveness of the Audio Information Protection for Determining the Identity of Virtual Speech Images // Proceeding of the Second International Conference on Security of Information and Networks. The Association for Computing Machinery. New York. 2009. – P. 235-239.
6. *Румянцев К.Е., Котенко С.В.* Идентификация личности на основе формирования оценки виртуального персонального образа // Информационное противодействие угрозам терроризма: Науч.-практ. журн. – 2006. – № 8. – С. 73-75.
7. *Котенко С.В.* Комплекс аурикулодиагностической идентификации // Информационное противодействие угрозам терроризма.: Науч.-практ. журн. – 2011. – № 16. – С. 73-79.
8. *Котенко В.В., Котенко С.В., Румянцев К.Е., Горбенко Ю.И.* Стратегия защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей // Прикладная радиоэлектроника. – 2013. – Т. 12, № 3. – С. 308-313.

Статью рекомендовал к опубликованию д.т.н., профессор И.Д. Горбенко.

**Котенко Станислав Владимирович** – Южный федеральный университет; e-mail: virtsecurity@mail.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: +78634315507; кафедра информационной безопасности телекоммуникационных систем; аспирант.

**Kotenko Stanislav Vladimirovich** – Southern Federal University; e-mail: virtsecurity@mail.ru; 2, Chekhov street, Taganrog, 347928, Russia; phone: +78634315507; the department of informative safety of the telecommunication systems; postgraduate student.