УДК 681.3

Анализ имитостойкости систем аутентификации сообщений с допустимостью погрешности передаваемых сигналов

Приведен анализ защищенности от подделки нового класса систем аутентификации с погрешностью и классической совершенной системы аутентификации без погрешности.

В. Г. Грибунин*, А. П. Мартынов, И. Н. Оков**

Существующие системы аутентификации сообщений, такие как криптографические системы формирования и проверки имитовставок и цифровых подписей, теряют свою способность к контролю подлинности при любой ошибке передачи их сигналов-носителей или кодограмм аутентификации [1]. Устранение этих недостатков возможно в новом классе систем аутентификации, способных контролировать подлинность передаваемых сообщений в условиях доставки их сигналами-переносчиками с некоторой допустимой погрешностью $\varepsilon_{доп} > 0$.

Рассмотрим защищенность от подделки систем аутентификации сообщений без допустимости погрешности и систем аутентификации с погрешностью, находящихся в одинаковых условиях. Для этого сравним систему аутентификации без погрешности, называемую $\mathcal{A}$-код, и систему аутентификации с погрешностью ε ($\mathcal{A}_\varepsilon$-код) при одинаковой энтропии $H(\mathcal{E})$ множества формируемых ими кодограмм аутентифицикации $\mathcal{E}$. В качестве $\mathcal{A}$-кода будем рассматривать алгоритм формирования и проверки имитовставок по ГОСТу 28147-89. Покажем, что при атаке имитации $\mathcal{A}_\varepsilon$-код способен обеспечить вероятность успешного обмана со стороны противника меньше, чем $\mathcal{A}$-код в тех же условиях.

Теорема 1. При фиксированной энтропии $H(E)$ множества кодограмм аутентифицикации $\mathcal{E}$ совершенная система аутентификации с отличной от нуля погрешностью ε кодирования сигналов-носителей сообщений обеспечивает вероятность обмана при атаке имитации $P_I(\mathcal{A}_\varepsilon$-код) меньше, чем вероятность $P_I(\mathcal{A}$-код) в совершенной системе аутентификации без погрешности при той же атаке противника.

* Генеральный штаб ВС РФ.

** Военная академия связи.

Доказательство. Из работы [2] известно, что для совершенных систем аутентификации без погрешности при атаке имитации выполняется равенство вида

$$\log_2 P_I(\mathcal{A}\text{-код}) = H(S) - H(E), \tag{1}$$

где $H(S)$ – энтропия множества сообщений.

Пусть в системе аутентификации сообщений с погрешностью ε кодирования их сигналоносителей предварительно множество сигналов сообщений S отображается во множество их аппроксимаций $\mathcal{U}$ с некоторой погрешностью $\varepsilon > 0$. Теория кодирования [3] определяет, что энтропия $H(U)$ множества аппроксимаций U равна ε-энтропии $H_\varepsilon(S)$ и справедливо строгое неравенство

$$H(S) > H(U) = H_\varepsilon(S). \tag{2}$$

В рассматриваемой системе аутентификации с погрешностью из предварительно сжатых с погрешностью ε сигналов сообщений источника S формируются кодограммы аутентификации множества $\mathcal{E}$ точно так же, как и в исходной системе аутентификации без погрешности. Для $\mathcal{A}_\varepsilon$ - кода, аналогично выражению (1), справедливо

$$\log_2 P_I\left(\mathcal{A}_\varepsilon\text{-код}\right) = H(U) - H(E). \tag{3}$$

Так как $H(S) > H(U)$, то

$$H(U) - H(E) < H(S) - H(E), \tag{4}$$

следовательно,

$$\log_2 P_I\left(\mathcal{A}_\varepsilon\text{-код}\right) < \log_2 P_I(\mathcal{A}\text{-код}), \tag{5}$$

и при $P_I < 1$ выполняется строгое неравенство

$$P_I\left(\mathcal{A}_\varepsilon\text{-код}\right) < P_I(\mathcal{A}\text{-код}), \tag{6}$$

что и требовалось доказать для совершенных систем аутентификации.

Данный результат может быть пояснен следующим образом. В теории аутентификации Симмонса для совершенных систем без погрешности доказано выполнение равенства [2]

$$P_I\left(\mathcal{A}_\varepsilon\text{-код}\right) = \frac{N_S}{N_E}, \tag{7}$$

где N_S – мощность множества сообщений источника, а N_E – мощность множества кодограмм аутентификации. После сжатия с погрешностью сообщений из множества S кодограммы аутентификации формируются из аппроксимаций множества $\mathcal{U}$. В совершенной системе аутентификации таких аппроксимаций справедливо

$$P_I\left(\mathcal{A}_\varepsilon\text{-код}\right) = \frac{N_U}{N_E}. \tag{8}$$

В системе с погрешностью число аутентифицируемых сжатых сообщений (мощность множества $\mathcal{U}$) строго меньше числа N_S, и поэтому вероятность успешной атаки имитации уменьшилась.

Следствие 2. При фиксированной энтропии кодограмм $H(E)$ при сжатии сигналов заверяемых сообщений с погрешностью ε в совершенной системе аутентификации при атаке имитации выполняется равенство

$$\frac{P_I(\mathcal{A}\text{-код})}{P_I(\mathcal{A}_\varepsilon\text{-код})} = 2^{\Delta I}, \tag{9}$$

где величина потери при сжатии по необратимой функции эпсилон-энтропия множества состояний источника $H_\varepsilon(S)$ меньше энтропии $H(S)$ на величину потери при сжатии количества информации ΔI, где $\Delta I > 0$:

$$\Delta I = H(S) - H_\varepsilon(S). \tag{10}$$

Доказательство. Перепишем выражения (1) и (3) в виде

$$H(S) = \log_2 P_I(\mathcal{A}\text{-код}) + H(E); \tag{11}$$

$$H(U) = \log_2 P_I(\mathcal{A}_\varepsilon\text{-код}) + H(E). \tag{12}$$

Подставляя выражения (11) и (12) в (10) с учетом $H(U) = H_\varepsilon(E)$, получаем

$$\Delta I = \log_2 P_I(\mathcal{A}\text{-код}) - \log_2 P_I(\mathcal{A}_\varepsilon\text{-код}). \tag{13}$$

Потенцируя обе части равенства (13) по основанию 2, завершим доказательство.

Таким образом, возможность потери некоторого количества информации ΔI при сжатии сигналов-носителей повышает защищенность заверяемых сообщений от подделки противником. Количественно оценим степень возможного повышения имитозащищенности. Обозначим энтропию на символ источника $H_0(S)$. Известно, что для стационарного эргодического источника S^k, генерирующего сообщения длиной k символов, выполняется равенство вида $H(S^k) = k\,H_0(S)$ [3]. Построим границу, определяющую пределы повышения имитозащищенности при атаке имитации при необратимом сжатии аутентифицируемых сообщений.

Следствие 3. При атаке имитации вероятность успешного обмана в совершенной системе аутентификации сообщений стационарного эргодического источника уменьшается при сжатии их сигналов-носителей с погрешностью $\varepsilon \le \varepsilon_{доп}$ в число раз

$$\frac{P_I(\mathcal{A}\text{-код})}{P_I(\mathcal{A}_\varepsilon\text{-код})} = 2^{k\{H_0(S) - R(\varepsilon)\}}, \tag{14}$$

где $R(\varepsilon)$ – функция скорости кодирования сигналов источника в зависимости от погрешности ε на символ источника, а аутентифицируемые сообщения состоят из k символов.

Для доказательства следствия 3 используются равенство (9) и определение функции скорости кодирования с погрешностью $R(\varepsilon)$ как наименьшего числа бит на символ источника при сжатии стационарного источника S с погрешностью ε на символ [3]. По определению $\Delta I = H(S^k) - R(\varepsilon) = H(S^k) - H_\varepsilon(S^k) = kH_0(S) - kH_\varepsilon(S) = k\{H_0(S) - H_\varepsilon(S)\}$, что завершает доказательство данного следствия: $\frac{P_I(\mathcal{A}\text{-код})}{P_I(\mathcal{A}_\varepsilon\text{-код})} = 2^{\Delta I} = 2^{H(S^k) - H_\varepsilon(S^k)} = 2^{k\{H_0(S) - R(\varepsilon)\}}$.

Интересно оценить, насколько велико может быть повышение имитозащищенности различных видов мультимедийных сообщений при их передаче. В соответствии с выражением (10) величина ΔI есть разница между энтропией $H(S)$ источника заверяемых сообщений и эпсилон-энтропией $H_\varepsilon(S)$ этого же источника. Для большинства реальных источников мультимедийных сообщений, которые требуется передавать с контролем их подлинности по каналам связи, вели-

чина $H_0(S) - H_\varepsilon(S)$ во много раз превышает величину $H_\varepsilon(S)$ при погрешности $\varepsilon \le \varepsilon_{доп}$, допустимой в соответствии с действующими требованиями к достоверности связи. Например, для речевых сообщений на один отсчет речи – в единицы – десятки раз, причем величина k составляет не менее тысяч отсчетов, для телевизионных сообщений на один пиксел – в десятки – сотни раз (k порядка тысяч – миллионов пикселов).

Пусть при передаче изображений для их дешифрования зрительной системой оператора их размеры составляют порядка $k \approx 24 \times 24$ пикселов. В работе [4] для 18 тестовых изображений, в которых яркость каждого пиксела представляется 8 битами, получена практически достижимая верхняя граница энтропии тестовых изображений: $\bar{H}_0(S) = 2{,}99$ бит/пиксел. Для сохранения требуемой дешифруемости изображений их допустимый коэффициент сжатия с потерями несущественной для получателя информации обычно составляет порядка 4–16 раз, т. е. практически реализуется скорость кодирования с погрешностью $R_{практ}(\varepsilon_{доп})$ от 2 до 0,5 бит/пиксел. В соответствии с полученным выражением определим, что аутентификация с погрешностью потенциально позволяет повысить имитозащищенность в $2^{k\{\bar{H}_0(S) - R(\varepsilon_{доп})\}} = 2^{24\times 24\{2{,}99-2\}} = 4{,}5 \cdot 10^{171}$ число раз при $R(\varepsilon_{доп}) = 2$ бит/пиксел.

Следовательно, необратимое сжатие сигналов заверяемых сообщений в системах аутентификации с погрешностью потенциально способно уменьшить вероятность имитонавязывания на много порядков, причем потенциальный выигрыш экспоненциально возрастает при использовании методов сжатия с меньшей скоростью кодирования и максимален при использовании в составе системы аутентификации алгоритма со скоростью кодирования $R(\varepsilon_{доп})$, равной эпсилон-энтропии $H_\varepsilon(S)$.

Следует подчеркнуть, что полученные в следствии 3 оценки повышения имитозащищенности не требуют использования идеальных методов сжатия заверяемых сообщений, т. е. позволяют практически реализовать доказанное повышение защищенности сообщений от навязывания ложной информации. Они позволяют оценить предельную величину дополнительной имитозащищенности в практически реализуемых системах аутентификации с ключом ограниченной длины, использующей реально применимые алгоритмы сжатия сигналов, по сравнению с системами передачи заверяемых сообщений без сжатия.

Например, в работе [5] показано, что речевой сигнал ИКМ со скоростью 64 кбит/с может быть сжат без потерь до скорости порядка 17–19 кбит/с. Следовательно, при частоте дискретизации речи 8 кГц практически достигнутая верхняя оценка энтропии речевого сигнала на один отсчет равна $\bar{H}_0(S) \approx 2{,}1$ бит/отсчет. Оценим, насколько использование существующих алгоритмов сжатия речевых сигналов с потерями в составе систем аутентификации речи позволяет повысить их имитозащищенность.

В каналах связи широко используется сжатие речевого сигнала с помощью адаптивной дельта-моделяции (АДМ) до скорости 16 кбит/с. Для АДМ скорость кодирования с погрешностью $\varepsilon \le \varepsilon_{доп}$ составляет $R_{АДМ}(\varepsilon_{доп}) = 2$ бит/отсчет. Для речепреобразующего устройства типа АТ-3001М в режиме формантного вокодера на скорости 1,2 кбит/с скорость кодирования составляет $R_{AT\text{-}3001M\text{-}1,2}(\varepsilon_{доп}) = 0{,}15$ бит/отсчет, а в режиме полосно-формантного вокодера на скорости 2,4 кбит/с – $R_{AT\text{-}3001M\text{-}2,4}(\varepsilon_{доп}) = 0{,}3$ бит/отсчет. У кодека речи стандарта GSM на скорости 13 кбит/с скорость кодирования составляет $R_{GSM}(\varepsilon_{доп}) = 1{,}625$ бит/отсчет. Пусть заверяется кадр речи, состоящий из 200 последовательных отсчетов: $k = 200$. По формуле (14) построим график (рис. 1), показывающий, насколько потенциально больше вероятность навязывания ложных рече-

вых кадров у системы имитозащиты без погрешности по сравнению с системой с погрешностью в зависимости от скорости кодирования заверяемой речи.

Из графика видно, что при использовании сжатия речи с потерями в АДМ вероятность навязывания ложных кадров речи потенциально можно уменьшить в 10^6 раз, встраивание кодека GSM в систему имитозащиты может дать потенциальный выигрыш в $3{,}9 \cdot 10^{28}$ раз, а использование формантного вокодера и полосно-формантного вокодера – в $2{,}3 \cdot 10^{108}$ и $2{,}5 \cdot 10^{117}$ раз соответственно. Следовательно, использование в каналах связи систем аутентификации сообщений с допустимостью погрешности их сигналов-носителей способно многократно повысить имитозащищенность их передачи.

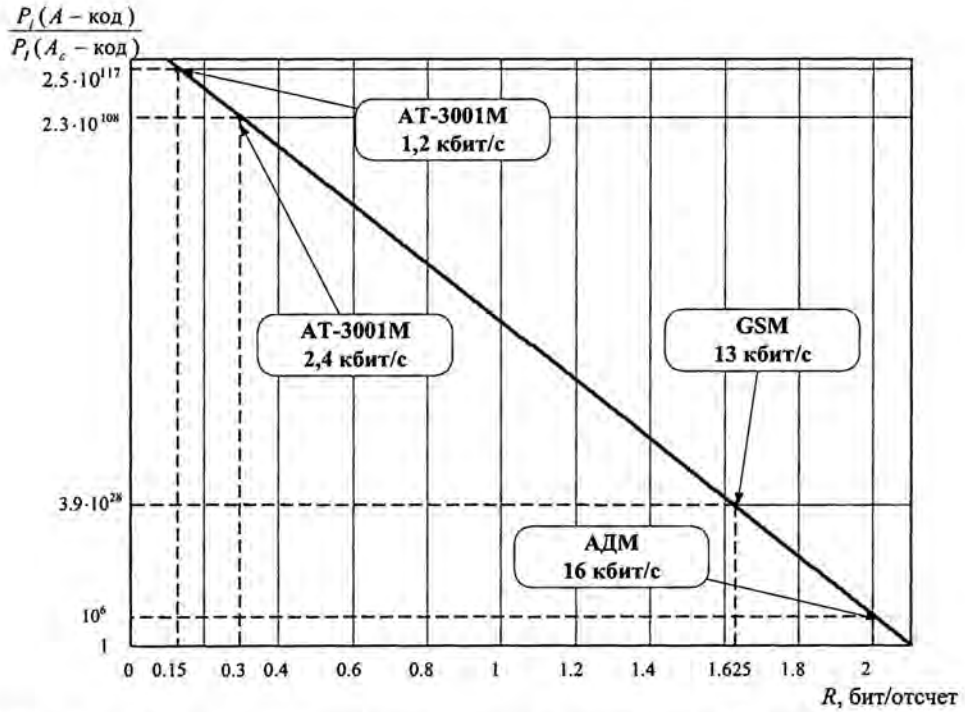

Рис. 1. Отношение вероятности навязывания ложных речевых кадров в атаке имитации системы имитозащиты без погрешности по сравнению с системой с погрешностью $\varepsilon_{\text{доп}}$ в зависимости от скорости кодирования заверяемой речи

В работе [2] доказывается, что зависимость $\log P_I(\mathcal{A}_\varepsilon\text{-код}) \geq H(S) - H(E)$ справедлива как для систем аутентификации без обеспечения секретности передаваемых сообщений, так и для систем с обеспечением их секретности, причем равенство достигается только в совершенных системах. Следовательно, доказанная теорема и следствия из нее справедливы для систем аутентификации сообщений с допустимостью погрешности их сигналов-носителей и для систем с обеспечением их секретности при атаке имитации. Для каналов связи характерна передача большого числа L заверенных сообщений в течение времени действия ключа аутентификации. Покажем, что при атаке подмены порядка L системы аутентификации с погрешностью, обеспечивающие секретность передаваемых сообщений, способны обеспечить вероятность успешного обмана со сто-

роны нарушитля меньше, чем системы аутентификации без погрешности при одинаковых условиях. Исследуем $O(L)$-секретные системы аутентификации сообщений, в которых в заданном порядке передается последовательность L преобразованных и имитозащищенных сообщений, и $U(L)$-секретные системы аутентификации сообщений, в которых эта последовательность неупорядочена [6].

Теорема 4. При фиксированной энтропии пространства ключей $H\left(V(\mathcal{A}\text{-код})\right)=$ $=H\left(V\left(\mathcal{A}_\varepsilon\text{-код}\right)\right)$ $O(L)$-секретная система аутентификации с отличной от нуля погрешностью ε кодирования сигналов сообщений стационарного эргодического источника уменьшает вероятность обмана при атаке подмены порядка $i=1,2,...,L$, где $1\le L\le N_S-1$, по сравнению с $O(L)$-секретной системой аутентификации сообщений без погрешности в число раз

$$\frac{P_{d_i}(\mathcal{A}\text{-код})}{P_{d_i}\left(\mathcal{A}_\varepsilon\text{-код}\right)}\le 2^{k\{H_0(S)-H_\varepsilon(S)\}}, \tag{15}$$

где N_S – мощность множества сообщений S.

Доказательство. Из работы [7] известно, что для систем аутентификации сообщений без погрешности ($\mathcal{A}$-код), удовлетворяющих требованию $O(L)$-секретности к чтению упорядоченных сообщений, при атаке подмены порядка L, где $1\le L\le N_S-1$, а N_S есть число возможных сообщений источника, справедливо соотношение

$$2^{H(V(A\text{-код}))}\ge 2^{H\left(S^L\right)}\prod_{i=1}^{L}\frac{1}{P_{d_i}(\mathcal{A}\text{-код})} \quad \text{для } 1\le i\le L, \tag{16}$$

где S^L – последовательность из L заверяемых сообщений.

Выражение (16) выполняется с равенством, если для $\mathcal{A}$-кода выполняется свойство L-минимальной ключевой энтропии, справедливо равенство $H\left(V/E^L\right)=H\left(S^L\right)$ и заверяемые сообщения равновероятны [7]. Здесь E^L есть последовательность из L кодограмм, полученных из данных сообщений на действующем ключе; $H\left(V(\mathcal{A}\text{-код})\right)$ – энтропия ключей аутентификации системы без погрешности. Из выражения (16) последовательно получим

$$H\left(V(\mathcal{A}\text{-код})\right)\ge H\left(S^L\right)-L\log P_{d_i}(\mathcal{A}\text{-код}) \quad \text{для } 1\le i\le L. \tag{17}$$

$$\log P_{d_i}(\mathcal{A}\text{-код})\ge\frac{1}{L}\left\{H\left(S^L\right)-H\left(V(\mathcal{A}\text{-код})\right)\right\}. \tag{18}$$

Пусть передаваемые сигналы-носители сжимаются с погрешностью ε на символ сообщения. В соответствии с теорией кодирования источников с погрешностью [3] последовательность L сигналов произвольного стационарного эргодического источника S^L может быть сжата со средней погрешностью ε на символ до предела $H_\varepsilon\left(S^L\right)$. При аутентификации таких сигналов с использованием того же множества ключей аутентификации $\mathcal{V}$ достижимая для противника вероятность имитонавязывания определяется как

$$\log P_{d_i}\left(\mathcal{A}_\varepsilon\text{-код}\right)\ge\frac{1}{L}\left\{H_\varepsilon\left(S^L\right)-H\left(V\left(\mathcal{A}_\varepsilon\text{-код}\right)\right)\right\}. \tag{19}$$

Так как по условию $H\left(V(\mathcal{A}\text{-код})\right) = H\left(V\left(\mathcal{A}_\varepsilon\text{-код}\right)\right)$, то из выражений (18) и (19) следует

$$H\left(S^L\right) - L\log P_{d_i}(\mathcal{A}\text{-код}) \geq H_\varepsilon\left(S^L\right) - L\log P_{d_i}\left(\mathcal{A}_\varepsilon\text{-код}\right); \tag{20}$$

$$L\left(\log P_{d_i}(\mathcal{A}\text{-код}) - \log P_{d_i}\left(\mathcal{A}_\varepsilon\text{-код}\right)\right) \leq H\left(S^L\right) - H_\varepsilon\left(S^L\right). \tag{21}$$

Для стационарного эргодического источника энтропия множества из L сигналов длиной k символов каждый выполняется равенство

$$H\left(S^L\right) = kH_0\left(S^L\right) = kLH_0(S), \tag{22}$$

где $H_0(S)$ – энтропия на один символ, а эпсилон-энтропия этого же множества сжатых с погрешностью сигналов равна

$$H_\varepsilon\left(S^L\right) = kLH_\varepsilon(S), \tag{23}$$

где $H_\varepsilon(S)$ – эпсилон-энтропия на один символ, т. е. минимально необходимое число битов для кодирования символа данного источника со средней погрешностью не более ε.

Подставляя выражения (22) и (23) в (21) и выполняя элементарные преобразования, получаем $\dfrac{P_{d_i}(\mathcal{A}\text{-код})}{P_{d_i}\left(\mathcal{A}_\varepsilon\text{-код}\right)} \leq 2^{\frac{1}{L}\left\{H_0\left(S^L\right) - H_\varepsilon\left(S^L\right)\right\}} = 2^{k\{H_0(S) - H_\varepsilon(S)\}}$, что и требовалось доказать.

Выражение (15) выполняется с равенством, если для исходной системы аутентификации выполняются свойства L-минимальной ключевой энтропии, $H\left(V/E^L\right) = H\left(S^L\right)$ и равномерного распределения множества сообщений, т. е. сравниваются совершенные системы аутентификации с погрешностью и без погрешности.

Таким образом, из доказанной теоремы следует, что чем сильнее можно сжать аутентифицируемые сообщения (чем больше разница $H_0(S) - H_\varepsilon(S)$), тем выше может быть их защищенность от подделки и что имитозащищенность экспоненциально растет с увеличением длины k аутентифицируемых сообщений, а это является новыми свойствами системы аутентификации с погрешностью. В частности, для известных систем аутентификации без погрешности защищенность от подделки не зависит от длины сообщений.

Доказанная для случая $O(L)$-секретных систем теорема также справедлива для $U(L)$-секретных систем аутентификации, в которых противник наблюдает множество из L кодограмм в произвольном порядке.

Следствие 5. При фиксированной энтропии пространства ключей $H\left(V\left(\mathcal{A}\text{-код}\right)\right) = H\left(V\left(\mathcal{A}_\varepsilon\text{-код}\right)\right)$ $U(L)$-секретная система аутентификации с отличной от нуля погрешностью ε кодирования сигналов сообщений стационарного эргодического источника уменьшает вероятность обмана при атаке подмены порядка $i = 1,2,...,L$, где $1 \leq L \leq N_S - 1$, по сравнению с $U(L)$-секретной системой аутентификации сообщений без погрешности в число раз

$$\frac{P_{d_i}(\mathcal{A}\text{-код})}{P_{d_i}\left(\mathcal{A}_\varepsilon\text{-код}\right)} \leq 2^{k\{H_0(S) - H_\varepsilon(S)\}}. \tag{24}$$

Доказательство данного следствия аналогично доказательству предыдущей теоремы и использует результаты, полученные в работе [7], в которых устанавливается, что для $U(L)$-секретных систем аутентификации выполняется выражение (16). Соответственно при выполнении свойств L-минимальной ключевой энтропии, $H\left(V/E^L\right)=H\left(S^L\right)$ и равномерного распределения множества сообщений $\left\{S^L\right\}$ справедливо строгое равенство в данном следствии, т. е. сравниваются совершенные системы аутентификации ($\mathcal{A}$-код) и ($\mathcal{A}_\varepsilon$-код).

Следствие 6. При фиксированной энтропии пространства ключей $H\left(V\left(A-\text{код}\right)\right)=$ $=H\left(V\left(A_\varepsilon-\text{код}\right)\right)$ $O(L)$- и $U(L)$-секретные системы аутентификации с отличной от нуля погрешностью $\varepsilon\le\varepsilon_{\text{доп}}$ кодирования сигналов-носителей сообщений стационарного эргодического источника уменьшают вероятность обмана при атаке подмены порядка $i=1,2,...,L$, где $1\le L\le N_S-1$, по сравнению с системами аутентификации без погрешности в число раз

$$\frac{P_{d_i}\left(\mathcal{A}\text{-код}\right)}{P_{d_i}\left(\mathcal{A}_\varepsilon\text{-код}\right)}\le 2^{k\{H_0(S)-R(\varepsilon)\}}, \tag{25}$$

где $R(\varepsilon)$ – практически достигнутая скорость кодирования сигналов заверяемых сообщений с погрешностью $\varepsilon\le\varepsilon_{\text{доп}}$, а $\varepsilon_{\text{доп}}$ – допустимая для получателя погрешность сигналов-носителей.

Заметим, что если в предыдущем следствии рассматривались системы аутентификации, в которых сигналы-носители сжимались до теоретически достижимой границы $H_\varepsilon(S)$, то в данном следствии исследуются системы аутентификации со сжатием сигналов до практически достижимой в реальных алгоритмах скорости кодирования $R(\varepsilon)$. Данная скорость может находиться в пределах $H_\varepsilon(S)\le R(\varepsilon)\le H_0(S)$. Если выполняется равенство $H_0(S)=R(\varepsilon)$, то сжатие с погрешностью отсутствует, нет и выигрыша по имитозащищенности. По мере приближения скорости $R(\varepsilon)$ кодирования реальных алгоритмов сжатия к величине эпсилон-энтропии $H_\varepsilon(S)$ экспоненциально растет имитозащищенность заверяемых сообщений, причем с ростом порядка атаки L степень повышения имитозащищенности остается постоянной.

Данное следствие позволяет оценить пределы повышения имитозащищенности сообщений, заверяемых системой аутентификации с погрешностью, использующей практически реализуемые алгоритмы сжатия. Например, пусть заверяются полутоновые изображения размером $n_x\times n_y=32\times32$, 128×96 (формат кадра SQCIF), 176×144 (QCIF), 352×288 пикселов (CIF). До сжатия яркость каждого пиксела изменяется в пределах 0...255, т. е. скорость источника равна 8 бит/пиксел. Известно [4], что типичные изображения сжимаются без искажений со средней скоростью порядка $R(\varepsilon=0)\ge H_0(S)=2{,}99$ бит/пиксел.

При оценке сжатия изображений обычно пользуются коэффициентом сжатия $K_{\text{сж}}$, который для различных изображений и алгоритмов сжатия может изменяться в пределах от единицы до нескольких сотен. Практически достижимую скорость кодирования заверяемых изображений с погрешностью $\varepsilon\le\varepsilon_{\text{доп}}$ удобно выразить в виде $R(\varepsilon)=\dfrac{8}{K_{\text{сж}}}$.

В соответствии с формулой (25) для различных размеров изображений и коэффициентов сжатия вычислим максимальные значения их имитозащищенности при использовании системы аутентификации с погрешностью

$$\frac{P_{d_i}(\mathcal{A}\text{-код})}{P_{d_i}(\mathcal{A}_\varepsilon\text{-код})} \le 2^{(n_x \times n_y)\{H_0(S)-R(\varepsilon)\}} = 2^{(n_x \times n_y)\left\{2{,}99-\frac{8}{K_{сж}}\right\}}.$$

На рис. 2 представлены пределы уменьшения вероятности навязывания ложных кадров изображения при атаке подмены порядка L. Для всех размеров кадров изображения при сжатии без потерь при $R(\varepsilon = 0) \ge H_0(S) = 2{,}99$ бит/пиксел повышение имитозащищенности отсутствует: $\frac{P_{d_i}(\mathcal{A}\text{-код})}{P_{d_i}(\mathcal{A}_\varepsilon\text{-код})} = 1$. Однако с ростом коэффициента сжатия неминуемо появляется погрешность сжатия ($\varepsilon > 0$) и имитозащищенность начинает увеличиваться по экспоненциальному закону. При малых размерах 32×32 пикселов и очень умеренной величине коэффициента сжатия $K_{сж} = 4$ вероятность навязывания ложных кадров может быть снижена в 2^{1000} раз. С ростом $K_{сж}$ и увеличением размера заверяемого кадра вероятность имитонавязывания ложных сообщений очень быстро уменьшается.

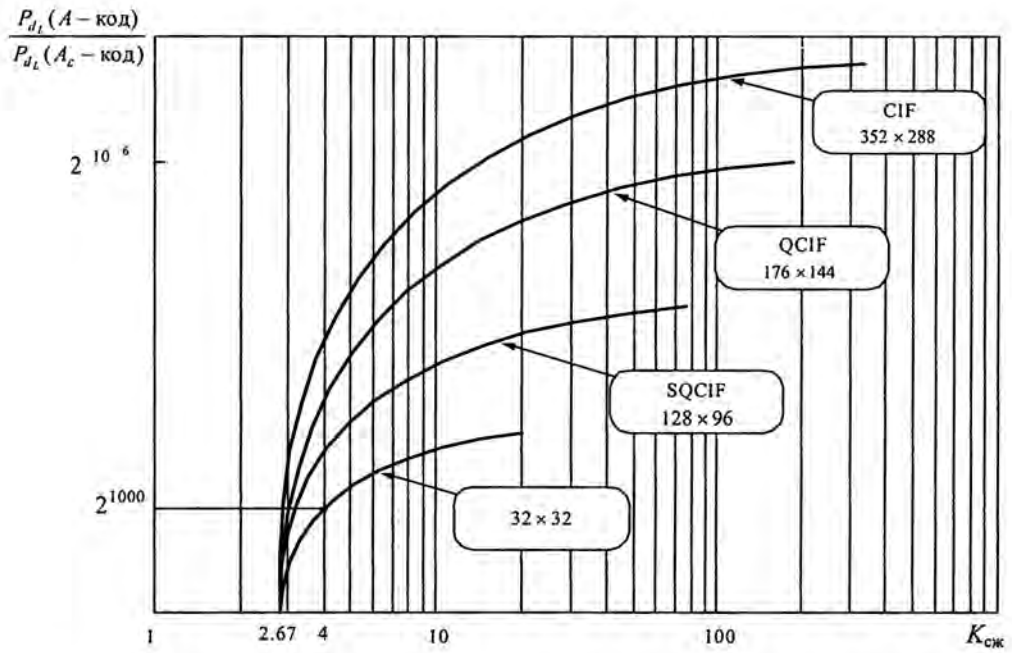

Рис. 2. Пределы уменьшения вероятности навязывания ложных кадров изображения при атаке подмены порядка L

Таким образом, контроль подлинности сжимаемых с погрешностью сигналов заверяемых мультимедийных сообщений, таких как видео и речь, способен существенно повысить их имитозащищенность при атаках имитации и подмены порядка L. Подчеркнем, что этот выигрыш получен благодаря допустимости для получателя сообщений погрешности их сигналов-носителей в пределах $\varepsilon \le \varepsilon_{доп}$. При этом разница между двумя сравниваемыми системами аутентификации

заключается в том, что в системе с погрешностью сигнал заверяемого сообщения допустимо необратимо сжимать с погрешностью $\varepsilon > 0$, что создает дополнительную неопределенность для нарушителя.

Список литературы

1. Оков И. Н. Криптографические системы аутентификации сообщений: оценки стойкости и требования к каналам передачи // Защита информации. Конфидент. 2001. № 5. С. 50–58.

2. Simmons G. J. Authentication theory/coding theory // Advances in Cryptology. Proc. CRYPTO-84. LNCS 196. Springer. 1985. P. 411–431.

3. Шеннон К. Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963.

4. Marvel L. Image Steganography for Hidden Communication // Thesis D. University of Delavare, 1999. P. 115.

5. Калинцев Ю. К. Разборчивость речи в цифровых вокодерах. М.: Радио и связь, 1991.

6. Зубов А. Ю. Совершенные шифры. М.: Гелиос АРВ, 2003.

7. Casse L. R., Martin K. M., Wild P. R. Bounds and characterizations of authentication/secrecy schemes // Design, codes and cryptography. 1998. Vol. 13, № 2. P. 107–129.

8. Волошин Н. П., Мартынов А. П., Николаев Д. Б., Фомченко В. Н. Алгоритмы криптографического преобразования. Симметрические и асимметрические криптографические системы и криптографические протоколы. Саров: «ИНФО», 2002.

Imitoresistance Analysis Message Authentification Systems With Admissible Error of Sending Signals

V. G. Gribunin, A. P. Martynov, I. N. Okov

The analysis of damage protection of new class of authentification systems with a error and the classical perfect authentification system without an error is resulted.