МАТЕМАТИЧЕСКИЕ МЕТОДЫ СТЕГАНОГРАФИИ

DOI 10.17223/20710410/15/5

УДК 681.511:3

МНОЖЕСТВА ИДЕНТИФИКАЦИОННЫХ НОМЕРОВ, УСТОЙЧИВЫЕ К АТАКЕ СГОВОРОМ

Т. М. Соловьёв, Р. И. Черняк

Национальный исследовательский Томский государственный университет, г. Томск, Россия

E-mail: tm.solovev@gmail.com, r.chernyack@gmail.com

Исследуются множества идентификационных номеров, обеспечивающие устойчивость стегосистемы к атаке сговором. Изучается структура таких множеств, различные способы представления, предлагается алгоритм их построения по ключу. Рассматривается задача идентификации участников атаки сговором.

Ключевые слова: *цифровые водяные знаки, стегосистемы идентификационных номеров, коллективные атаки, атака сговором.*

Введение

В настоящее время для защиты медиаконтента от несанкционированного использования широко применяются цифровые водяные знаки (ЦВЗ). В общем случае ЦВЗ — это некоторые метки, внедряемые в исходный материал. Они могут содержать информацию о времени и месте производства контента, а также о пользователе, которому этот контент предназначался. Метки последнего типа выделяются в отдельный класс и называются идентификационными номерами (ИН).

В случае применения ИН в контейнер, предназначенный каждому пользователю, внедряется персональный номер, позволяющий контролировать дальнейший путь этого контейнера. Такие системы в работе [1] называются *стегосистемами идентификационных номеров*. Если пользователь окажется медиапиратом и начнет незаконное распространение контента, то ИН позволит быстро определить злоумышленника. При этом предполагается, что все контейнеры одинаковы, то есть выданные копии отличаются только в тех позициях, в которые внедрены идентификаторы. Одной из основных отличительных черт данных систем является их потенциальная уязвимость к *коллективным атакам*, или *атакам сговором*. При реализации таких атак используются особенности стегосистем ИН, поэтому обеспечение защиты с помощью классических для ЦВЗ методик невозможно.

В работах [2, 3] рассматривались проблемы создания множеств ИН, устойчивых к коллективным атакам. Настоящая работа обобщает и расширяет полученные ранее результаты. Подробно исследуется структура множеств ИН, приводятся их основные характеристики. Обсуждается проблема идентификации группы злоумышленников при помощи ИН, полученного в результате атаки сговором. В заключение приводится алгоритм построения множества ИН по ключу.

1. Основные определения

Рассмотрим стегосистему ИН с множеством идентификаторов W. Пусть среди пользователей системы существует группа злоумышленников, обладающих копиями контента с идентификаторами из множества P.

Определение 1. *Атакой сговором* называется следующая последовательность действий:

1) определение части позиций, в которые внедрен ИН, посредством побитного сравнения копий, имеющихся у злоумышленников;
2) создание новой копии путем изменения значений бит с номерами, определенными на шаге 1.

Идентификатор, содержащийся в копии, полученной в результате атаки сговором, далее будем называть *ложным*.

Возможны следующие угрозы:

а) создание копии с ИН, не идентифицирующим никого;
б) создание копии с ИН из множества $W \setminus P$, то есть с идентификатором одного из пользователей, непричастных к атаке.

Из определения 1 непосредственно следует, что атака сговором более эффективна в случае, если ИН в разных копиях внедрен в разные позиции. Поэтому с точки зрения защиты целесообразно внедрение идентификаторов в одинаковые позиции во всех копиях. Далее рассматриваются только такие стегосистемы.

Замечание 1. Ложный ИН, независимо от фиксации бит на шаге 2 атаки сговором, находится внутри наименьшего интервала, покрывающего множество идентификаторов использованных копий.

Последний факт является важной особенностью атаки сговором, и на его основе представляется возможным разработать эффективное противодействие данной атаке.

Определение 2. Множество идентификационных номеров $W_n \subseteq \{0,1\}^n$ (или W, если длина ИН не существенна) называется *допустимым*, если каждому его непустому подмножеству P взаимно-однозначно сопоставляется наименьший интервал $I(P)$, покрывающий это подмножество.

Далее, если не оговорено другое, будем рассматривать только собственные подмножества P множества W_n. Интервал $I(P)$ будем называть *соответствующим* множеству P и обозначать троичным вектором с компонентами из множества $\{0,1,-\}$. При этом внутренние компоненты интервала обозначаются символом «$-$», а внешние — соответствующими константами из $\{0,1\}$.

В рамках решаемой задачи достаточно ограничиться рассмотрением таких допустимых множеств W_n, для которых $I(W_n) = \underbrace{-\,-\,\ldots\,-}_{n}$. В противном случае все ИН и, как следствие, все покрывающие интервалы содержат одну и ту же константу в некоторой компоненте, что никак не помогает при идентификации сговорившихся, а лишь вносит избыточность во внедряемую метку.

2. Свойства допустимых множеств

Свойство 1. Множество W допустимо, если и только если для любого его подмножества P интервал $I(P)$ не содержит векторов из $W \setminus P$.

Доказательство. Необходимость. Если вектор w из $W \setminus P$ принадлежит интервалу $I(P)$, то $I(P) = I(P \cup \{w\})$, что противоречит допустимости множества W, поскольку $P \neq P \cup \{w\}$.

Достаточность[1]. Пусть W не является допустимым, т. е. существуют два его различных подмножества P_1 и P_2, такие, что $I(P_1) = I(P_2)$. Пусть для определенности $P_1 \setminus P_2$ не пусто. Возьмём вектор w из $P_1 \setminus P_2$. Он принадлежит P_1, следовательно, принадлежит и $I(P_1) = I(P_2)$. Таким образом, интервал $I(P_2)$ содержит вектор из $P_1 \setminus P_2 \subseteq W \setminus P_2$. ■

Свойство 1 означает, что если множество идентификаторов стегосистемы ИН является допустимым, то злоумышленники при проведении атаки сговором никогда не смогут «подставить» невиновного пользователя, и любое множество с таким свойством допустимо.

Лемма 1. Пусть W — допустимое множество, $|W| \geqslant 3$, $P \subseteq W$, $|P| \geqslant 2$. Тогда $\dim(I(P)) \geqslant |P|$, где $\dim(I)$ — размерность интервала I.

Доказательство. Индукция по мощности множества P.

Б а з а и н д у к ц и и. $|P| = 2$. Покажем, что для любых двух различных векторов w_p и w_q из W размерность покрывающего их интервала не может быть равна единице. Предположим противное: w_p отличается от w_q только в одной компоненте. Пусть она имеет номер i. Рассмотрим вектор $w_r \in W$, отличный от w_p и w_q (он существует, так как $|W| \geqslant 3$). Возможны два варианта: либо $w_r[i] = \overline{w_p[i]} = w_q[i]$, либо $w_r[i] = w_p[i] = \overline{w_q[i]}$. В первом случае получим $I(\{w_p, w_q, w_r\}) = I(\{w_p, w_r\})$, во втором — $I(\{w_p, w_q, w_r\}) = I(\{w_q, w_r\})$. Оба варианта противоречат определению допустимого множества.

Ш а г и н д у к ц и и. Пусть для любого P мощности n верно неравенство $\dim(I(P)) \geqslant n$. Рассмотрим произвольное подмножество $P' \subseteq W$ мощности $n+1$. Оно может быть представлено в виде $P' = P \cup \{w\}$, где $|P| = n$, $w \in W \setminus P$. Интервал $I(P \cup \{w\})$ либо равен интервалу $I(P)$, либо имеет бóльшую размерность. Первое невозможно в силу допустимости W, следовательно, $\dim(I(P')) \geqslant \dim(I(P)) + 1 \geqslant n + 1 = |P'|$. ■

Следствием леммы является следующее свойство.

Свойство 2. Мощность допустимого множества W_n не превышает n.

Данное свойство налагает суровое ограничение на количество пользователей системы. Например, для того чтобы обеспечить идентификационными номерами сеть из десяти миллионов пользователей, необходимо использовать ИН длиной не менее мегабайта. Такой объем дополнительного материала является существенным, и его дальнейшее увеличение может создавать проблемы на этапе внедрения метки.

Свойство 3. Множество W_n мощности n допустимо, если и только если оно является сферой радиуса 1 с некоторым вектором a в качестве центра, т. е. имеет вид $O_1(a) = \{x \in \{0,1\}^n : \mathrm{d}(a,x) = 1\}$, где $\mathrm{d}(a,x)$ — расстояние по Хэммингу между векторами a и x.

Доказательство. Необходимость для $n \leqslant 2$ проверяется непосредственно.

Пусть $n > 2$. Построим вектор a для произвольного допустимого множества W_n мощности n. Обозначим различные $(n-1)$-элементные подмножества W_n через P_1, P_2, …, P_n. Согласно лемме 1, $\dim(I(P_i)) \geqslant n-1$ для всех $i = 1, 2, \ldots, n$, а так как $\dim(I(W_n)) = n$ и существует только один интервал размерности n, то $\dim(I(P_i)) = n-1$, $i = 1, 2, \ldots, n$. Следовательно, для каждого i существует единственное j_i, такое, что j_i-я компонента во всех векторах из P_i одинакова. Запишем её значение

[1] Достаточность данного свойства сформулирована и доказана Р. С. Стружковым.

в j_i-ю компоненту вектора a; заметим, что $j_i \neq j_k$ при $i \neq k$ ввиду $\dim(I(W_n)) = n$. По построению, $\mathrm{d}(a, w) = 1$ для любого $w \in W_n$, т. е. $W_n = O_1(a)$.

Достаточность. Покажем, что для любых различных P_1 и P_2 — подмножеств $O_1(a)$ — верно неравенство $I(P_1) \neq I(P_2)$. Очевидно, что если $|P_1| = 1$ или $|P_2| = 1$, то $I(P_1) \neq I(P_2)$. Пусть $|P_1| > 1$, $|P_2| > 1$ и $P_1 \setminus P_2 \neq \varnothing$. Возьмём вектор $w \in P_1 \setminus P_2$; пусть i — номер компоненты, в которой w отличается от a. Так как все векторы в $O_1(a)$, за исключением w, совпадают в i-й компоненте, то i-я компонента в $I(P_2)$ будет внешней, а в $I(P_1)$ — внутренней. Таким образом, $I(P_1) \neq I(P_2)$. ■

Пусть $W = \{w_i : i = 1, 2, \ldots, k\}$; обозначим $W^+(l) = \{w_i \cdot a_i : w_i \in W,\ a_i \in \{0,1\}^l,\ i = 1, 2, \ldots, k\}$, где символом «$\cdot$» обозначена операция конкатенации.

Свойство 4. Если W — допустимое множество, то все множества вида $W^+(l)$ также являются допустимыми для любых l.

Доказательство. От противного: пусть существует l, такое, что для некоторых двух различных $P_1^+(l), P_2^+(l) \subseteq W^+(l)$ верно равенство $I\left(P_1^+(l)\right) = I\left(P_2^+(l)\right)$. Тогда $I(P_1) = I(P_2)$ для соответствующих $P_1, P_2 \subseteq W$, что противоречит допустимости множества W. ■

3. Матричное представление множеств ИН

Рассмотрим множество ИН W_n мощности k. Представим его в виде булевой матрицы $W_{k\times n}$, строками которой будут векторы из множества W_n:

$$W_{k\times n} = \begin{pmatrix} w_1[1] & w_1[2] & \ldots & w_1[n] \\ w_2[1] & w_2[2] & \ldots & w_2[n] \\ \vdots & \vdots & \ddots & \vdots \\ w_k[1] & w_k[2] & \ldots & w_k[n] \end{pmatrix}.$$

Матрицы, соответствующие допустимым множествам, будем также называть допустимыми.

Определим следующие операции над матрицами:

1) перестановка столбцов или строк;
2) инверсия всех элементов заданного столбца;
3) удаление одного из повторяющихся столбцов или добавление столбца, равного одному из уже присутствующих в матрице.

Определение 3. Матрицы M и M' назовем *эквивалентными*, если они могут быть получены друг из друга путем применения операций 1–3. Множества ИН W и W' назовем *эквивалентными*, если соответствующие им матрицы эквивалентны.

Очевидно, что применение к матрице операций 1–3 не влияет на ее допустимость, и матрица, эквивалентная допустимой, также является допустимой.

Утверждение 1. Матрица $W_{k\times n}$ является допустимой, если и только если она эквивалентна блочной матрице вида $(E_k M)$, где E_k — единичная матрица размера $k\times k$; M — произвольная k-строчная матрица.

Доказательство. Необходимость. Пусть допустимой матрице $W_{k\times n}$ соответствует множество $W_n = \{w_1, w_2, \ldots, w_k\}$. Определим два индексных множества $K = \{1, 2, \ldots, n\}$ и $J = \varnothing$.

Рассмотрим интервал $I_1 = I(W_n \setminus \{w_1\})$. Пусть I_1 имеет l внешних компонент с номерами i_1, i_2, …, i_l. Тогда вектор w_1 в этих компонентах отличается от остальных

векторов множества W_n, т. е. матрица $W_{k\times n}$ имеет вид

$$\begin{pmatrix} c_{11} & c_{12} & \dots & \boxed{\overline{c_{i_1}}} & \dots & \boxed{\overline{c_{i_2}}} & \dots & \boxed{\overline{c_{i_l}}} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{i_1} & \dots & c_{i_2} & \dots & c_{i_l} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{k1} & c_{k2} & \dots & c_{i_1} & \dots & c_{i_2} & \dots & c_{i_l} & \dots & c_{kn} \end{pmatrix}.$$

Поскольку матрица булева, выделенные столбцы равны с точностью до инверсии, следовательно, удаление всех этих столбцов, за исключением одного, есть эквивалентное преобразование. Исключим из множества K элементы $i_2, i_3, \dots, i_l$, а элемент i_1 добавим в множество J.

Проведем аналогичные действия для векторов $w_2, w_3, \dots, w_k$; заметим, что множества номеров внешних компонент интервалов $I(W_n \setminus \{w_i\})$, $i = 1, 2, \dots, k$, попарно не пересекаются.

В результате будут построены множества J и K, такие, что

$$J \subseteq K, \quad |J| = k. \tag{1}$$

Составим матрицу $\widetilde{W}_{k\times n'}$ из тех столбцов матрицы $W_{k\times n}$, номера которых входят в множество K. По построению, $\widetilde{W}_{k\times n'}$ эквивалентна $W_{k\times n}$, следовательно, является допустимой. Выделим в $\widetilde{W}_{k\times n'}$ подмножество столбцов, номера которых образуют множество J. Эти столбцы имеют следующий вид:

$$\left(\underbrace{\overbrace{c_{i_j}, c_{i_j}, \dots, c_{i_j}}^{j-1}, \overline{c}_{i_j}, c_{i_j}, \dots, c_{i_j}}_{k}\right)^{\mathrm{T}}, \quad j = 1, 2, \dots, k.$$

Эквивалентными преобразованиями матрица, составленная из таких столбцов, может быть приведена к E_k. Остальные столбцы образуют матрицу M. Если $n' = k$, матрица M пуста.

Достаточность. Матрица E_k допустима по свойству 3, следовательно, по свойству 4 матрица $(E_k M)$ (и любая эквивалентная ей) также является допустимой. ■

Замечание 2. Для любой допустимой матрицы размера $k \times n$ существует эквивалентная ей блочная матрица вида $(E_k M_{k\times m})$, где $0 \leqslant m \leqslant n - k$.

Следствие 1. Для любой допустимой матрицы размера $k \times n$ существует эквивалентная блочная матрица вида $(E_k M)$, в которой подматрица M либо пуста, либо не является допустимой.

Доказательство. По утверждению 1, любая допустимая матрица эквивалентными преобразованиями может быть приведена к виду $(E_k M_{k\times m})$. Рассмотрим подматрицу $M_{k\times m}$.

Если $m < k$, то матрица $M_{k\times m}$ либо пуста, либо не допустима (по свойству 2).

Пусть $m \geqslant k$ и матрица $M_{k\times m}$ допустима. Тогда, с учетом замечания 2, эквивалентными преобразованиями она может быть приведена к виду $(E_k M_{k\times t})$ для $0 \leqslant t \leqslant m-k$, т. е. исходная матрица примет вид $(E_k E_k M_{k\times t})$, и одно из вхождений E_k может быть удалено. Получим $(E_k M_{k\times t})$.

Те же рассуждения применим к матрице $M_{k\times t}$ и так далее, пока за конечное число шагов не будет получена эквивалентная исходной матрица вида $(E_k M_{k\times s})$, где $0 \leqslant s \leqslant m - lk$, $0 \leqslant l \leqslant [m/k]$, и подматрица $M_{k\times s}$ либо пуста, либо не допустима. ■

Утверждение 1 позволяет ввести понятие базы допустимого множества.

Определение 4. *Базой* (*базовой частью*) k-строчной допустимой матрицы называется набор таких её k столбцов, из которых может быть составлена матрица, эквивалентная E_k. Совокупность остальных столбцов матрицы называется *дополнением* (*дополнительной частью*).

Определение 5. Допустимая матрица называется *сильно допустимой*, если удаление из неё любого столбца влечет потерю свойства допустимости. Множество, соответствующее такой матрице, будем также называть *сильно допустимым*.

Утверждение 2. Допустимая матрица является сильно допустимой, если и только если она состоит только из базовой части.

Доказательство. Необходимость. Пусть для некоторой k-строчной сильно допустимой матрицы W существует эквивалентная матрица $(E_k M)$, причем подматрица M не пуста. Удалим из W один из дополнительных столбцов. В результате получим матрицу W', для которой найдется эквивалентная матрица $(E_k M')$. По утверждению 1, W' допустима, что противоречит предположению сильной допустимости W.

Достаточность очевидна. ■

Таким образом, свойство допустимости равносильно наличию подматрицы, эквивалентной единичной матрице заданного размера. Оставшаяся часть матрицы не влияет на допустимость и может быть выбрана произвольно.

4. Построение допустимых множеств

Построение допустимого множества, которому соответствует единичная матрица, не вызывает никаких сложностей, однако на практике этого недостаточно. Необходим алгоритм, с помощью которого можно построить любое допустимое множество. Поскольку в реальных стегосистемах количество идентификаторов и их размеры велики, важным фактором является производительность алгоритма. Для обеспечения возможности распараллеливания алгоритм должен обладать следующим свойством: каждый вектор строится независимо от остальных.

Алгоритм 1 Построение допустимого множества

Вход: $k, n, v, \pi, M_{k\times(n-k)}$
Выход: допустимое множество W из k векторов длины n

1: $i := 1$, w — нулевой вектор длины n, $W := \varnothing$
2: **Пока** $i \leqslant k$
3: $\quad w[i] := 1$
4: $\quad$ **Для** $j := k+1$ до n
5: $\quad\quad w[j] := M[i, j]$
6: $\quad w := w \oplus v$
7: $\quad$ Переставить компоненты вектора w в соответствии с подстановкой π
8: $\quad$ Добавить w в W
9: $\quad i := i + 1$, обнулить w
10: **Вернуть** W

Результатом работы алгоритма является множество из k идентификационных номеров длины n ($n \geqslant k$). Номера столбцов, которые в соответствующей матрице необходимо инвертировать, задаются булевым вектором v длины n. Для изменения порядка следования столбцов используется перестановка $\pi \in S_n$. Пара (v, π) может быть ис-

пользована в качестве ключа. На вход алгоритма подаётся также матрица M размера $k \times (n-k)$, которая вносит в идентификационные номера некоторую избыточность.

Согласно утверждению 1, матрица, соответствующая любому допустимому множеству, может быть построена из матрицы вида $(E_k M)$ при помощи операций перестановки, инвертирования и добавления/удаления повторяющихся столбцов. Таким образом, с помощью алгоритма 1 может быть построено любое допустимое множество.

5. Идентификация злоумышленников

Обсудим проблему идентификации участников сговора по полученному ими ложному ИН. В соответствии со свойством 1, в случае использования допустимого множества ложный ИН никогда не совпадет ни с одним из существующих в системе идентификаторов. Таким образом, для множества ИН W_n задача идентификации может быть сформулирована следующим образом: «Используя ложный ИН w' из $\{0,1\}^n \setminus W_n$, восстановить некоторое непустое подмножество пользователей, участвовавших в атаке сговором».

Пусть, для наглядности, допустимое множество задано матрицей E_k. В этом случае в идентификаторе каждого пользователя есть только одна единица. Она находится в первой компоненте ИН первого пользователя, во второй компоненте ИН второго и так далее. Таким образом, если у злоумышленников нет i-го ИН, то в i-й компоненте построенного ими ложного идентификатора всегда будет ноль. Другими словами, если в i-й компоненте ложного ИН присутствует единица, это однозначно говорит о том, что i-й пользователь участвовал в сговоре. На основе этих рассуждений представляется возможным идентифицировать некоторое непустое подмножество участников сговора по построенному ими ложному ИН во всех случаях, кроме одного — когда последний целиком состоит из нулей.

Рассмотрим пример атаки сговором с участием трёх злоумышленников на множество ИН, заданное матрицей E_5; пусть злоумышленниками являются первые три пользователя:

$$\begin{pmatrix} \boxed{\begin{matrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{matrix}} \\ \begin{matrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{matrix} \end{pmatrix}.$$

Ложные идентификаторы в этом случае выбираются из интервала $---00$. Ниже показан результат идентификации злоумышленников в зависимости от построенного ими ложного ИН:

Ложный ИН	Результат идентификации
11000	$\{1,2\}$
10100	$\{1,3\}$
01100	$\{2,3\}$
11100	$\{1,2,3\}$
00000	$\varnothing$

Заметим, что во всех случаях, кроме последнего, найдено некоторое подмножество злоумышленников, при этом ни один не причастный к атаке пользователь не был обвинён. Очевидно, что подобные рассуждения возможны и в том случае, если некоторые столбцы в матрице E_k будут инвертированы. В рассмотренном примере, инвертируя

первый и второй столбцы, получим матрицу

$$\left(\begin{array}{|ccccc|} \hline 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ \hline 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array} \right).$$

В этом случае результат идентификации будет следующим:

Ложный ИН	Результат идентификации
00000	$\{1, 2\}$
01100	$\{1, 3\}$
10100	$\{2, 3\}$
00100	$\{1, 2, 3\}$
11000	$\varnothing$

В общем случае вывод о том, что i-й пользователь участвовал в атаке сговором, делается, если в i-й компоненте ложного ИН наблюдается значение $\overline{f_{\text{maj}}}(w_1[i], w_2[i], \ldots, w_k[i])$, где f_{maj} — мажоритарная функция:

$$f_{\text{maj}}(x) = \begin{cases} 1, & \text{если } \sum\limits_{i=1}^{n} x_i > n/2 \ , \\ 0 & \text{иначе.} \end{cases}$$

Используя метод из доказательства необходимости в утверждении 1, в матрице, задающей допустимое множество, всегда можно выделить базовую часть. Таким образом, описанный способ идентификации злоумышленников может быть использован в любом допустимом множестве.

6. Мажорирующая атака

В предложенном методе идентификации используются лишь те компоненты ложного ИН, которые соответствуют базовым столбцам, поэтому далее ограничимся рассмотрением только сильно допустимых множеств.

В приведенных примерах идентификации присутствует ложный ИН, который не идентифицирует никого:

$$w[i] = f_{\text{maj}}(w_1[i], w_2[i], \ldots, w_k[i]), \quad i = 1, 2, \ldots, n.$$

Обозначим его w_{maj}. Возникает вопрос, всегда ли злоумышленники могут построить w_{maj} и существует ли стратегия, позволяющая им получать именно этот ИН, а не какой-то случайный вектор из интервала, соответствующего использованным идентификаторам?

Утверждение 3. Если множество W сильно допустимо, $P \subseteq W$ и $|P| \geqslant 2$, то $w_{\text{maj}} \in I(P)$.

Доказательство. Заметим, что в сильно допустимом множестве для любых двух различных его элементов w_s и w_t и для любого $i = 1, 2, \ldots, n$ всегда выполняется следующее: либо $w_s[i] \neq w_t[i]$, либо $w_s[i] = w_t[i] = w_{\text{maj}}[i]$. Другими словами, каждая компонента интервала $I(\{w_s, w_t\})$ либо внутренняя, либо совпадает с соответствующей компонентой w_{maj}, следовательно, $w_{\text{maj}} \in I(\{w_s, w_t\})$. Таким образом, для любого $P \subseteq W$ мощности не меньшей двух $w_{\text{maj}} \in I(P)$. ■

Замечание 3. Идентификационный номер w_{maj} может быть построен следующим образом:

$$w_{\text{maj}}[i] = f_{\text{maj}}(w_p[i], w_q[i], w_r[i]), \quad i = 1, 2, \ldots, n,$$

где w_p, w_q, w_r — любые попарно различные ИН из сильно допустимого множества W.

Таким образом, при наличии трех или более ИН возможно построение метки, не идентифицирующей никого.

Описанный способ построения ложного ИН назовём *мажорирующей атакой*. В соответствии с предложенным методом идентификации проведение данной атаки является единственным способом для злоумышленников избежать ответственности. Поскольку мажорирующая атака состоит в выборе конкретного вектора из $I(P)$, возможна разработка метода эффективного противодействия данной атаке.

Заключение

В работе предлагается модель множеств идентификаторов для стегосистем ИН, позволяющая противостоять атаке сговором. Последнее достигается за счет уникальности наименьших покрывающих интервалов для каждого непустого подмножества идентификаторов. Выделен ряд свойств таких множеств, исследована их структура и предложен алгоритм генерации. Задача идентификации злоумышленников по ИН, полученному в результате сговора, решена для всех коллективных атак, за исключением одного частного случая — мажорирующей атаки. Противостояние последней является одним из приоритетных направлений дальнейшего исследования. Данная задача может быть решена с использованием статистических методов, поскольку, в рамках предложенной модели, возможен произвольный выбор дополнительной части.

ЛИТЕРАТУРА

1. *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография. М.: Солон-Пресс, 2002.
2. *Струйжков Р. С., Соловъёв Т. М., Черняк Р. И.* Цифровые водяные знаки, устойчивые к атаке сговором // Прикладная дискретная математика. Приложение. 2009. № 1. С. 56–59.
3. *Соловъёв Т. М., Черняк Р. И.* Стегосистемы идентификационных номеров, устойчивые к атаке сговором // Прикладная дискретная математика. Приложение. 2010. № 3. С. 41–44.