УДК 519.7

О ПРИМЕНЕНИИ КОДОВ ХЭММИНГА В СИСТЕМЕ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ДЛЯ КОНФЕРЕНЦИЙ В МНОГОПОЛЬЗОВАТЕЛЬСКИХ СИСТЕМАХ СВЯЗИ

В. М. Деундяк, А. А. Таран

ФГНУ «НИИ «Спецвузавтоматика»
Южный федеральный университет

Поступила в редакцию 23.05.2015 г.

Аннотация. На основе общего подхода В. М. Сидельникова рассматривается кодовая система распределения ключей в многопользовательских системах связи, обеспечивающая безопасность при наличии в этом сообществе коалиции злоумышленников, мощность которой не превышает некоторого заранее предусмотренного порога. В случае превышения этого порога описываются атаки на систему, среди атак выделяются эффективные и осторожные, и строятся модели атак. Для систем, построенных на кодах Хэмминга, вычисляется вероятность успешного проведения атак.
Ключевые слова: системы распределения ключей для конференций, коалиционные атаки, коды Хэмминга.
Annotation. The article discusses code-based key distribution systems within the approach of V. M. Sidelnikov. These systems are secure against coalition attacks if number of traitors in coalition is less than system specific threshold. In case when number of traitors in coalition is greater than this threshold models of coalition attacks are suggested. In case of systems based on Hamming codes probabilities of successful attacks are presented.
Keywords: conference key distribution systems, coalition attack, Hamming codes.

ВВЕДЕНИЕ

Практически значимые задачи проектирования систем защиты информации для распределенных вычислительных сетей и построения различных интегрированных систем безопасности предполагают создание защищенных многопользовательских систем связи для безопасного обмена данными (см., например, [1], [2], [3]). Многие криптографические протоколы, используемые при создании таких систем, требуют наличия у участников общего секретного ключа [1], и поэтому взаимодействующие стороны должны заранее договариваться о таком ключе. В связи с этим актуальной является задача генерации и распределения ключей в сообществе на основе использования открытых компьютерных сетей. В ряде работ эта задача решается с помощью техники помехоустойчивого кодирования [4], [5]; в книге В. М. Сидельникова ([6], с. 286) этот теоретико-кодовый подход систематизирован и обобщен. Между участниками обмена данными распределяется некоторая ключевая информация, на основе которой они могут самостоятельно вычислить необходимые общие секретные ключи конференций. Такие теоретико-кодовые системы распределения ключей могут нормально функционировать даже при наличии в сообществе злоумышленников, цель которых – использование секретной информации во вред сообществу. Однако системой распределения ключей заранее предполагается, что количество злоумышленников должно быть ограничено некоторым однозначно определяемым порогом, а в случае превышения этого порога система перестает быть устойчивой к атакам злоумышленников.

Представляется актуальным исследовать эффективность работы кодовых систем распределения ключей в случае превышения предусмотренного порога числа злоумышленников по аналогии с тем, как это сделано в задаче о коалициях злоумышленников в системах специального широковещательного шифрования [7].

В настоящей работе строятся алгоритмические модели работы сервера распределения ключей и создания участниками общего секретного ключа для конференции, а также модель атаки на ключ конференции, которую может провести коалиция злоумышленников. В процессе классификации атак выделено два новых признака: эффективность и осторожность; к эффективным атакам относятся те, которые осуществляются за полиномиальное время, а к осторожным – те, при которых злоумышленники себя не обнаруживают. Для системы защиты с порогом 1, построенной на кодах Хэмминга, в работе вычислены вероятности возможности осуществления эффективных и осторожных атак в случае превышения порога числа злоумышленников.

2. КОДОВАЯ СИСТЕМА РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Предположим, что в сообществе $X = \{x_1; \dots x_N\}$ из $|X| = N$ участников имеется необходимость создания конференций и защищенного обмена данными внутри конференции по открытым каналам связи. Эту задачу будем решать с помощью системы, в которой генерацией и распределением секретных ключей для участников сообщества занимается какой-либо доверенный сервер, а секретный ключ конференции создается с использованием своих секретных ключей каждым участником конференции индивидуально. В этом разделе в рамках подхода В. М. Сидельникова строится модель работы сервера, модель создания ключа конференцией и описывается мера эффективности системы распределения ключей.

Модель работы сервера. Рассмотрим сервер, у которого имеется проверочная матрица H_C используемого в системе базового $[n,k]_q$-кода $C(\subset F_q^n)$, где F_q^n – линейное пространство векторов длины n над полем Галуа F_q, q – степень простого числа, k – размерность кода. Матрица H_C имеет размеры $s \times n$, где $s = n - k$. Базовый код выбирается таким, чтобы его длина n была не меньше мощности сообщества N. Для определения ключевого пространства F_q^u выбирается параметр u так, чтобы его значение существенно превышало $n: u \gg n$. Сервер действует по следующему алгоритму.

1. Каждому пользователю x_i сервер присваивает идентификационный номер $\overline{a}_i = (a_{i,1}, \dots, a_{i,s}) \in F_q^s$, который выбирается из столбцов проверочной матрицы H_C. Далее идентификационные номера используются в качестве открытых ключей и могут отождествляться с пользователями x_i.

2. Для конференций мощности t сервер генерирует множество

$$\Xi^{(t)} = \left\{ \overline{\xi}_{i_1,\dots,i_t} \in F_q^u \mid 1 \le i_1 \le i_2 \le \dots \le i_t \le s \right\}$$

линейно-независимых секретных ключей, при этом $\left|\Xi^{(t)}\right| = C_{s+t-1}^t \ll u$.

3. Для каждого пользователя x_i с идентификационным номером $\overline{a}_i = (a_{i,1}, \dots, a_{i,s})$ сервер вычисляет набор

$$\Xi^{(t,\overline{a}_i)} =$$

$$= \left\{ \overline{\xi}_{i_1,\dots,i_{t-1}}(\overline{a}_i) \in F_q^u \mid 1 \le i_1 \le i_2 \le \dots \le i_{t-1} \le s \right\} \subset F_q^u$$

секретных ключей по формуле:

$$\overline{\xi}_{i_1,\dots,i_{t-1}}(\overline{a}_i) = \sum_{j=1}^{s} a_{i,j} \overline{\xi}_{i_1,\dots,i_{t-1},j}, \quad 1 \le i_1 \le i_2 \le \dots \le i_{t-1} \le s \qquad (1)$$

Отметим, что $\left|\Xi^{(t,\overline{a}_i)}\right| = C_{s+t-2}^{t-1}$.

После того, как сервер разошлет пользователям сгенерированные для них ключи, его роль в распределении ключей заканчивается. В дальнейшем он может выступать, например, в качестве хранилища открытых ключей.

Модель создания общего секретного ключа конференцией. Предположим, что t пользователей системы с идентификационными номерами $\overline{a}_{j_1}, \dots, \overline{a}_{j_t}$ по открытым каналам договариваются о проведении конференции T. Для обеспечения защищенного общения внутри этой конференции они генерируют общий секретный ключ, для этого

каждый из участников $\overline{a}_{j_\lambda}$ вычисляет общий секретный ключ с помощью своего набора секретных ключей $\Xi^{(t,\overline{a}_{i_\lambda})}$ и открытых ключей (идентификационных номеров) других участников $\overline{a}_{j_1},\ldots,\overline{a}_{j_t}$ по следующей формуле:

$$\overline{k}_{\overline{a}_{j_1},\ldots,\overline{a}_{j_t}} =$$

$$= \sum_{i_1,\ldots,i_{\lambda-1},i_{\lambda+1},\ldots,i_t=1}^{s} a_{j_1,i_1}\ldots a_{j_{\lambda-1},i_{\lambda-1}} a_{j_{\lambda+1},i_{\lambda+1}}\cdots \quad (2)$$

$$\cdots a_{j_t,i_t}\overline{\xi}_{i_1,\ldots,i_{\lambda-1},i_{\lambda+1},\ldots,i_t}(\overline{a}_{j_\lambda}).$$

Отметим, что результат вычисления будет одним и тем же для всех участников конференции и при этом будет зависеть от открытых ключей каждого из них ([6], с. 292).

Мера эффективности системы распределения ключей. В [4], [6] в качестве меры эффективности системы используется оценка на размер ключей, которые необходимо хранить каждому пользователю. В наших обозначениях эта мера может быть записана в виде:

$$D = \left|\Xi^{(t,\overline{a}_i)}\right| \cdot \log_2 \left|F_q^u\right| = C_{s+t-2}^{t-1} \cdot u \cdot \log_2 q.$$

Чем меньше значение D, тем более эффективной считается система. В [6], с. 297, отмечается, что кодовые системы распределения ключей являются наиболее эффективными при использовании кодов Рида – Соломона в качестве базовых кодов.

3. АТАКИ НА СИСТЕМУ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

В этом разделе рассматриваются внутренние атаки на кодовую систему распределения ключей, т.е. такие атаки на ключи конференций, которые могут осуществить недобросовестные члены сообщества (злоумышленники). Выделено два новых признака – эффективность и осторожность и построена модель атаки на ключ конференции

Коалиции злоумышленников. Находящиеся в сообществе злоумышленники могут объединиться в коалицию, распространив между собой свои наборы секретных ключей. Ключ $\overline{k}_T$ конференции T называется скомпрометированным коалицией злоумышленников W, если

$$\overline{k}_T \in L\left(\bigcup_{\overline{a}_i \in W} \Xi^{(t,\overline{a}_i)}\right),$$

где $L(Y)$ – линейная оболочка множества Y $\left(\subset F_q^u\right)$.

Системой распределения ключей для конференций с t участниками, обеспечивающей безопасность в присутствии произвольной коалиции из w злоумышленников (или (t,w)-системой), называется система, в которой ключ любой конференции T размера t не может быть скомпрометированным никакой из коалиций злоумышленников W, размера не большего, чем порог w, и такой, что $T \cap W = \varnothing$. Приведем в удобном для дальнейшего виде важный результат из теории (t,w)-систем (см. [6], с. 294–296).

Теорема 1. Кодовая система защиты является (t,w)-системой тогда и только тогда, когда любые различные $w+1$ столбцов проверочной матрицы H_C линейно-независимы над полем F_q. Ключ $\overline{k}_T$ конференции T является скомпрометированным коалицией злоумышленников W тогда и только тогда, когда хотя бы у одного участника конференции идентификационный номер принадлежит $L(W)$, т. е. $T \cap L(W) \neq \varnothing$.

Атаки на ключ конференции. Целью внутренней атаки на ключ конференции является вычисление коалицией злоумышленников этого ключа для ознакомления с передаваемыми на конференции сообщениями.

Зафиксируем конференцию T, коалицию злоумышленников W и рассмотрим событие

$$A = A(T,W) := "T \cap L(W) \neq \varnothing",$$

состоящее в том, что ключ $\overline{k}_T$ конференции T скомпрометирован коалицией злоумышленников W. В случае наступления события A злоумышленники могут вычислить секретные ключи любого из пользователей $\overline{a} \in T \cap L(W)$ по следующей формуле:

$$\xi_{i_1,\ldots i_{t-1}}(\overline{a}) = \sum_{\overline{b} \in W} \alpha_{\overline{b}} \cdot \xi_{i_1,\ldots,i_{t-1}}(\overline{b}), \quad (3)$$

где коэффициенты α_b находятся из представления

$$\overline{a} = \sum_{\overline{b} \in W} \alpha_{\overline{b}} \cdot \overline{b}. \quad (4)$$

Такую атаку будем называть *эффективной*. Вычислив набор секретных ключей поль-

зователя $\overline{a}$ по формулам (3), (4) (за полиномиальное время, например, с помощью метода Гаусса), коалиция злоумышленников может, используя (2), получить в итоге ключи для всех конференций, в которых $\overline{a}$ принимает участие.

В случае, когда злоумышленники из коалиции не в состоянии провести эффективную атаку, они могут подобрать ключ конференции $\overline{k}_T$ полным перебором множества всех потенциально возможных ключей. Так как $\overline{k}_T \in F_q^u$, то им придется перебрать q^u возможных ключей. Такую атаку будем называть *неэффективной*. Время и объем перебора могут контролироваться в системе распределения ключей с помощью увеличения параметра u.

Отметим, что в результате атаки возможно не только пассивное ознакомление с передаваемыми на конференции сообщениями, но и какое-то его другое использование, например, нелегальное распространение. В этом случае факт нелегального использования ключа конференции может быть обнаружен. При предположении, что размер коалиции не превышает установленного теоремой 1 порога, ключ конференции может быть реально получен только участниками этой конференции. Поэтому в случае обнаружения нелегального использования ключа подозрение в первую очередь падет на самих участников этой конференции. Введем событие

$$B = B(T, W) := "W \cap T = \varnothing",$$

которое означает, что ни один из членов коалиции не является участником атакуемой конференции, и выделим два вида атак: неосторожные и осторожные. Атаку назовем *неосторожной*, если событие B не выполняется, т. е. если какой-то участник коалиции является участником конференции и может легально получить ключ конференции. Отметим, что все неосторожные атаки могут быть проведены эффективно. Атаку назовем *осторожной*, когда выполняется событие B, т. е. когда ни один из участников коалиции не является участником атакуемой конференции, и тогда ни на одного из злоумышленников подозрение напрямую не падет. Отметим, что неэффективные атаки бывают только осторожными.

Введем событие $C = A \cap B$, соответствующее возможности проведения осторожной эффективной атаки. Отметим, что в случае, когда мощность коалиции злоумышленников не превышает определенный теоремой 1 допустимый порог, система предоставляет защиту от осторожных эффективных атак, т.к. проведение таких атак в этом случае невозможно.

Теперь построим алгоритм, которому может следовать коалиция злоумышленников W для того, чтобы вычислить секретные ключи конференций.

1. Получив от сервера ключи, коалиция проверяет выполнение события B для интересующих их конференций T. Когда событие B не наступает, т. е. когда, по крайней мере, один из злоумышленников является участником конференции T, то ключ $\overline{k}_T$ вычисляется злоумышленниками легально. Таким образом, в этом случае возможна неосторожная эффективная атака.

2. Если же событие B наступает, и, следовательно, возможны осторожные атаки, то коалиция проверяет выполнение события A, т. е. методом Гаусса проверяет возможность представления открытого ключа одного из членов конференции T в виде (4). Если событие A наступает, то наступает и событие $C = A \cap B$. В этом случае коалиция способна осуществить осторожную эффективную атаку.

3. Если же событие A не наступает, то возможна только осторожная неэффективная атака, для осуществления которой коалиции придется перебирать q^u возможных ключей конференции T.

4. ПРИМЕНЕНИЕ КОДОВ ХЭММИНГА В СИСТЕМЕ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Рассмотрим семейство кодов Хэмминга с проверочными матрицами H_s, у которых столбцы являются двоичными представлениями чисел от 1 до 2^{s-1}, s – натуральное число ([8], с. 64). У кодов Хэмминга длина $n = 2^s - 1$,

размерность $k = 2^s - s - 1$, минимальное кодовое расстояние $d = 3$. Например,

$$H_4 = \begin{pmatrix} 0000000011111111 \\ 0001111100001111 \\ 0110011001100 11 \\ 1010101010101 01 \end{pmatrix}.$$

Любые два столбца матрицы H_s являются линейно-независимыми, поэтому если построить описанную ранее систему распределения ключей для сообщества из N пользователей на кодах Хэмминга, то она окажется $(t,1)$-системой, т. е. рассчитанной на защиту только от одного злоумышленника.

Рассмотрим задачу оценки вероятностей компрометации ключа конференции размера t в случае превышения допустимого порога, а именно вычислим вероятности возможности проведения эффективных и осторожных эффективных атак.

Предположим, что в сообществе из $N = 2^s - 1$ участников имеется коалиция злоумышленников W, $|W| = w (> 0)$. Сервер случайно и равномерно распределяет между членами сообщества открытые и секретные ключи по правилу, описанному в разделе 2. Предположим, что произвольным образом создается конференция T, $|T| = t$. Для расчета вероятностей наступления событий A и C нам понадобятся гипотезы о размерности линейных подпространств, порожденных наборами идентификационных номеров коалиций злоумышленников.

Зафиксируем натуральные числа d и w. Через $H_{d,w}$ обозначим событие, состоящее в том, что при случайном равновероятном выборе коалиции W мощности $|W| = w$ выполняется равенство: $\dim(L(W)) = d$. Впоследствии эти гипотезы позволят нам определить число членов сообщества, ключи которых может вычислить коалиция. Вероятности $p(H_{d,w})$ будем вычислять рекуррентно. Непосредственно из определения вытекает:

$$p(H_{1,1}) = 1, \quad p(H_{d,1}) = 0 \quad (d \neq 1),$$

$$p(H_{1,w}) = 0 \quad (w \neq 1).$$

Остальные вероятности вычисляются в следующем утверждении.

Лемма 1. Рассмотрим систему распределения ключей на кодах Хэмминга. Пусть $w \geq 2$, $d \geq 2$. Тогда имеет место следующая рекуррентная формула:

$$p(H_{d,w}) = \frac{p(H_{d-1,w-1}) \cdot (n - (2^{d-1} - 1))}{n - (w-1)} + \frac{p(H_{d,w-1}) \cdot (2^d - w)}{n - (w-1)}. \quad (5)$$

Доказательство. Предположим, что известно число элементарных исходов, благоприятствующих гипотезам $H_{d-1,w-1}$ и $H_{d,w-1}$. Обозначим их $|H_{d-1,w-1}|$ и $|H_{d,w-1}|$ соответственно. Чтобы получить систему W из w векторов с $\dim(L(W)) = d$, достаточно добавить к некоторой системе W' из $w-1$ векторов с размерностью $\dim(L(W'))$ равной $d-1$ или d один вектор: в первом случае – линейно-независимый от остальных, а во втором – линейно-зависимый. Для первого случая число таких векторов вычисляется по формуле

$$|F_2^s \setminus L(W')| = n - (2^{d-1} - 1),$$

а для второго — по формуле:

$$|L(W') \setminus (W' \cup \{\bar{0}\})| = 2^d - 1 - (w-1) = 2^d - w.$$

С помощью этих формул получаем рекуррентную формулу для вычисления числа элементарных исходов, благоприятствующих гипотезе $H_{d,w}$:

$$|H_{d,w}| = \frac{|H_{d-1,w-1}| \cdot (n - (2^{d-1} - 1))}{w} + \frac{|H_{d,w-1}| \cdot (2^d - w)}{w}.$$

Так как $p(H_{d,w}) = \frac{|H_{d,w}|}{C_n^w}$, то

$$p(H_{d,w}) = \frac{C_n^{w-1} \cdot p(H_{d-1,w-1}) \cdot (n - (2^d - 1))}{C_n^w \cdot w} + \frac{C_n^{w-1} \cdot p(H_{d,w-1}) \cdot (2^d - w)}{C_n^w \cdot w}.$$

Раскрыв и сократив биномиальные коэффициенты, получим (5). •

Воспользуемся (5) и вычислим вероятности возможности проведения эффективной и осторожной эффективной атак коалицией, т. е. вероятности наступления событий A и C для случайных конференций и коалиций.

Теорема 2. Зафиксируем натуральные числа t и w. Тогда: 1) вероятность наступления события A для случайно и равновероятно выбранных коалиции W мощности w и конференции T мощности t вычисляется по формуле

$$p(A)=\sum_{d=1}^{s} p(A\mid H_{d,w})\cdot p(H_{d,w}), \qquad (6)$$

где

$$p(A\mid H_{d,w})=\sum_{i=1}^{\min\{t,\tilde{w}\}}\frac{C_{\tilde{w}}^{i}\cdot C_{n-\tilde{w}}^{t-i}}{C_{n}^{t}}, \qquad (7)$$

2) вероятность наступления события C для случайно и равновероятно выбранных коалиции W мощности w и конференции T мощности t вычисляется по формуле

$$p(C)=\sum_{d=1}^{s} p(C\mid H_{d,w})\cdot p(H_{d,w}), \qquad (8)$$

где

$$p(C\mid H_{d,w})=\sum_{i=1}^{\min\{t,\tilde{w}-w\}}\frac{C_{\tilde{w}-w}^{i}\cdot C_{n-\tilde{w}}^{t-i}}{C_{n}^{t}}, \qquad (9)$$

а

$$\tilde{w}:=\left|L(W)\setminus\{0\}\right|=2^{d}-1$$

– количество пользователей системы, ключи которых могут быть вычислены коалицией злоумышленников W.

Доказательство. Теорему можно получить из леммы 1 и формулы полной вероятности ([9], с. 122). Действительно, рассмотрим первое утверждение. Набор $\{H_{d,w}\}_{d=1}^{s}$ является совокупностью взаимоисключающих событий, одно из которых обязательно произойдет, т. к. размерность линейной оболочки системы векторов $W\in F_2^s$ не может быть больше s и меньше 1. По формуле (7) вычисляется вероятность попадания в случайную конференцию хотя бы одного пользователя с идентификационным номером из $L(W)$ при условии, что $\deg(L(W))=d$. Каждое слагаемое в этой сумме – вероятность попадания в случайную конференцию ровно i пользователей системы, секретные ключи которых есть у коалиции злоумышленников, т. е. пользователей с идентификационными номерами из $L(W)$ – вычисляется по формуле для гипергеометрического распределения вероятностей ([9], стр. 55). Применив формулу полной вероятности, получим (6).

Аналогично доказывается второе утверждение. •

Результаты вычислений. По приведенным выше формулам можно построить графики зависимости вероятности наступления событий A и C от числа злоумышленников в коалиции. Так как эти события характеризуют возможность проведения атак на ключи случайных конференций, то вероятности их наступления совпадают с долей всех возможных конференций, на ключи которых коалиция может провести соответствующие атаки.

Рассмотрим графики, построенные для параметров ($s=7,\ t=5$) и ($s=7,\ t=6$). Сравнивая эти две пары графиков, можно увидеть, что увеличение размера конференции ведет к увеличению вероятности атак.

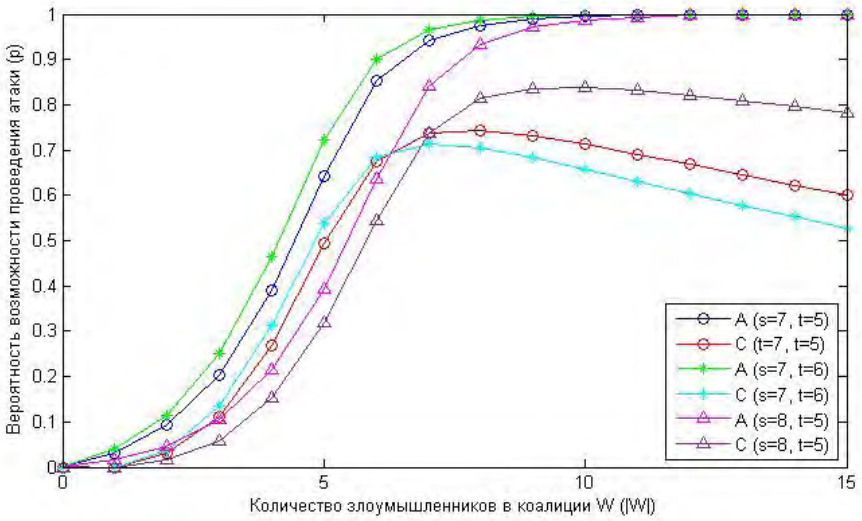

Рис.1. Изменение значений вероятностей событий A и C в зависимости от s и t

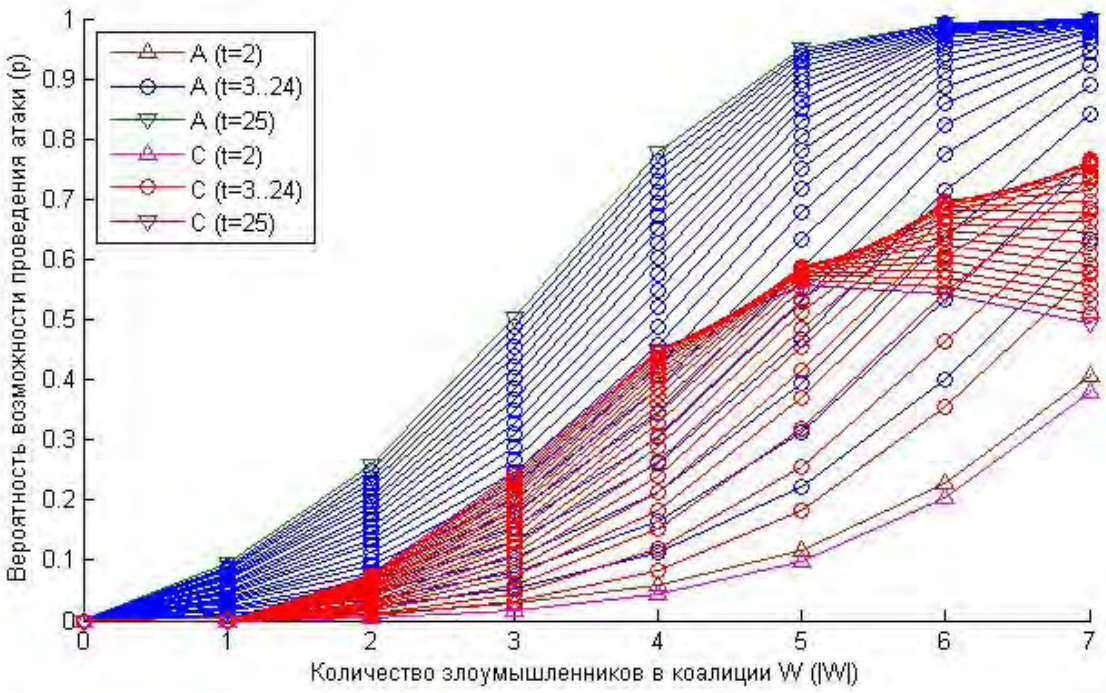

Рис. 2. Общий вид графиков значений вероятностей

Увеличение размера сообщества (если сравнивать графики, соответствующие параметрам ($s=7,\ t=5$) и ($s=8,\ t=5$) приведет к уменьшению вероятностей атак.

На рис. 2 изображены графики вероятностей проведения атак для параметров $s=8$ и t в диапазоне [2; 25]. Изучение этих графиков позволяет предложить дополнительную меру защиты. Так как увеличение размера конференций t ведет к увеличению вероятности возможности проведения атак при небольших размерах коалиций w, то ведение ограничений на размеры конференций позволяет ограничивать вероятности проведения атак.

5. ОСОБЕННОСТИ ПРИМЕНЕНИЯ РС-КОДОВ В СИСТЕМЕ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Как было отмечено ранее, наиболее эффективными системами распределения ключей, т. е. системами, в которых пользователям будет необходимо хранить минимально возможное число ключей, являются системы, построенные на кодах Рида – Соломона. Но если исследовать поведение этой системы в случае превышения допустимого порога числа злоумышленников аналогично тому, как было сделано в разделе 4 для кодов Хэмминга, то окажется, что если размер коалиции превысит порог хотя бы на одного злоумышленника, то коалиция сможет провести эффективную атаку на ключ любой конференции, так как сможет вычислить наборы секретных ключей всех участников сообщества.

Действительно, рассмотрим проверочную матрицу кода Рида–Соломона ([8], стр. 235)

$$H=\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(q-2)} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(q-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{q-k-1} & \alpha^{(q-k-1)2} & \dots & \alpha^{(q-k-1)(q-2)} \end{pmatrix}.$$

Любые $(q-k-1)$ столбцов матрицы H являются линейно-независимыми, т. к. представляют из себя матрицу, полученную произведением матрицы Вандермонда на невырожденную диагональную матрицу, составленную из ненулевых α^i. Отсюда по теореме 1 получаем, что система распределения ключей, построенная на коде Рида – Соломона, гарантирует защиту от коалиций размера не более, чем $(q-k-1)-1$. Но если в коалиции будет $(q-k-1)$ злоумышленников, то совокупность их идентификационных номеров образует базис в линейном пространстве, порожденном столбцами матрицы H.

Поэтому коалиция сможет вычислить наборы секретных ключей всех участников сообщества и провести атаку на ключ любой конференции, как показано в разделе 3.

Таким образом, система, построенная на кодах Рида – Соломона, является эффективной, но *неустойчивой*, т.к. превышение предусмотренного порога приводит к возможности атаки на ключ любой конференции с вероятностью 1. Представляется полезным выяснить, какие коды, с одной стороны, могут, как коды Рида – Соломона, предоставлять защиту от большого числа злоумышленников и при этом требовать не очень большой размер ключей и, с другой стороны, мягко реагировать на превышения допустимого порога мощности коалиции злоумышленников как коды Хэмминга.

СПИСОК ЛИТЕРАТУРЫ

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М. : ТРИУМФ, 2002. – 816 с.

2. *Кащенко А. Г.* Многокритериальная модель выбора варианта системы защиты информации для распределенной вычислительной сети предприятия / А. Г. Кащенко // Вестник Воронежского ун-та. Серия: Системный анализ и информационные технологии. – 2010. – № 2. – С. 46–49.

3. *Дурденко В. А., Рогожин А. А.* Разработка классификации и архитектуры построения интегрированных систем безопасности / В. А. Дурденко, А. А. Рогожин // Вестник Воронежского ун-та. Серия: Системный анализ и информационные технологии. – 2013. – №1. – С. 61–70.

4. *Blom R.* An optimal class of symmetric key generation systems / R. Blom // Advances in Cryptology. LNCS. – 1985. – V. 209. – P. 335–338.

5. *Blundo C., Mattos L.A.F., Stinson D. R.* Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution / C. Blundo, L. A. F. Mattos, D. R. Stinson // Advances in Cryptology. LNCS. – 1996. – V. 1109. – P. 387–400.

6. *Сидельников В. М.* Теория кодирования / В. М. Сидельников. – М.: ФИЗМАТЛИТ, 2008. – 324 с.

7. *Деундяк В. М., Мкртичян В. В.* Исследование границ применения схемы защиты информации, основанной на РС-кодах / В. М. Деундяк, В. В. Мкртичян // Дискретный анализ и исследование операций. – 2011. – Т. 18, №3. – С. 21–38.

8. *Деундяк В. М., Маевский А. Э., Могилевская Н. С.* Методы помехоустойчивой защиты данных / В. М. Деундяк, А. Э. Маевский, Н. С. Могилевская – Ростов-на-Дону : ЮФУ, 2014. – 309 с.

9. *Феллер В.* Введение в теорию вероятностей и её приложения. Т. 1 / В. Феллер – М. : МИР, 1964. – 498 с.

Деундяк В. М. – кандидат физико-математических наук, доцент кафедры «Алгебра и дискретная математика», Южный федеральный университет; старший научный сотрудник ФГНУ «НИИ «Спецвузавтоматика», г. Ростов-на-Дону.
E-mail: vlade@math.rsu.ru.

Таран А. А. – магистрант, кафедра «Алгебра и дискретная математика», Южный федеральный университет, г. Ростов-на-Дону.
E-mail: fraktal-at@yandex.ru.

Deundyak V. M. – Candidate of Physical and Mathematical Sciences, Associate professor of the department of Algebra and Discrete Mathematics, Southern Federal University; Senior Scientist of FSSO «SRI «Spetsvuzavtomatika», Rostov-on-Don.
E-mail: vlade@math.rsu.ru.

Taran A. A. – Student of the Southern Federal University, department of Algebra and Discrete Mathematics, Rostov-on-Don.
E-mail: fraktal-at@yandex.ru.