УДК 519.676
DOI: 10.24160/1993-6982-2017-6-152-157

Об информационной скорости в схемах предварительного распределения ключей с взаимно дополняющими условиями их корректности

А.В. Затей

Приведены схемы предварительного распределения ключей, использующиеся для уменьшения общего объема секретной информации, доставляемой абонентам сети по защищенным каналам, с помощью которой вычисляется секретный ключ для установления безопасного сетевого соединения между участниками. Схемы предварительного распределения ключей в компьютерной сети предусматривают формирование доверенным центром на основе исходной секретной системной ключевой информации пакетов, одинаковых по объему, и пересылку их соответствующим участникам. При этом состав пакетов и дополнительная несекретная информация о них публикуются на общедоступном сервере. Полученная каждым участником ключевая информация должна быть достаточной для вычисления рабочих ключей для связи с участниками той или иной группы из числа групп, в которые он входит, и состав пакетов секретной информации которых ему известен. Состав самих групп также общеизвестен и опубликован.

С помощью компьютерных экспериментов, а также минимальных и достаточных оценок вероятностного алгоритма синтеза схем предварительного распределения ключей с условиями корректности двух схем (KDP, Key Distribution Pattern и HARPS, Hashed Random Preloaded Subset Key Distribution) показано как теоретическое, так и практическое преимущество комбинированной схемы с точки зрения эффективности. Рассмотрено понятие информационной скорости как критерия эффективности схемы предварительного распределения ключей в задаче минимизации распределяемого объема секретной информации, хранимой участниками сети.

Ключевые слова: информационная скорость, вероятностный метод синтеза, схема предварительного распределения ключей, криптографическая хеш-функция, условие корректности, компьютерная сеть.

Для цитирования: Затей А.В. Об информационной скорости в схемах предварительного распределения ключей с взаимно дополняющими условиями их корректности // Вестник МЭИ. 2017. № 6. С. 152—157. DOI: 10.24160/1993-6982-2017-6-152-157.

On the Information Rate in Key Pre-Distribution Schemes with Mutually Complementary Correctness Conditions

A.V. Zatey

The article presents the key pre-distribution schemes that are used to reduce the total amount of secret information distributed to network subscribers through secure channels, using which the secret key is calculated to establish a secure network connection between the participants. The key pre-distribution schemes in a computer network imply the use of a trusted center that produces packets having the same volume and transmits them to the relevant participants proceeding from the original secret system key information. The composition of these packets and additional unclassified information about them are published on a public server. The secret key information received by each participant must be sufficient for calculating the working keys to communicate with the participants of a certain group from among the groups the participant belongs to and who knows the composition of their secret information packets. The composition of the groups themselves is also commonly known and published.

Computer experiments were carried out, and the minimal and sufficient assessments were performed using the probabilistic algorithm for synthesizing key pre-distribution schemes with the correctness conditions of two well-known schemes, namely, the Key Distribution Pattern (KDP) and Hashed Random Preloaded Subset Key Distribution (HARPS), and it has been shown from the obtained results that the combined scheme has advantages — both in theoretical and practical respects — in regard of its efficiency. The information rate concept is considered as an efficiency criterion of a key pre-distribution scheme in the task of minimizing the distributed volume of secret information stored by the network participants.

Key words: information rate, probabilistic method of synthesis key pre-distribution scheme, cryptographic hash function, correctness condition, computer network.

For citation: Zatey A.V. On the Information Rate in Key Pre-Distribution Schemes with Mutually Complementary Correctness Conditions. MPEI Vestnik. 2017; 6:152—157. (in Russian). DOI: 10.24160/1993-6982-2017-6-152-157.

Проанализирована эффективность и проведено сравнение схем предварительного распределения ключей с взаимно дополняющими условиями корректности.

Для соединения в безопасном режиме (создания и обновления общей закрытой информации на сервере) стороны должны обладать секретными ключами, которые доставляются по защищенным каналам. Для уменьшения общего количества закрытой информации существуют известные методы предварительного распределения, когда стороны вычисляют секретные ключи, используя предварительно полученную ключевую информацию и общедоступную информацию с сервера.

Для уменьшения вероятности ошибки при передаче информации по защищенным каналам желательно минимизировать объем, хранимый участниками сети, и сократить объем передачи. Данный подход характеризуется понятием информационной скорости схемы [1]. Схема предварительного распределения ключей тем эффективнее, чем меньше секретной информации передается по защищенному каналу.

Схемы предварительного распределения ключей в компьютерной сети предусматривают формирование доверенным центром на основе исходной секретной системной ключевой информации пакетов, одинаковых по объему, секретных единиц ключевой информации для каждого участника сети и пересылку этих пакетов соответствующим участникам. При этом состав этих пакетов и, возможно, дополнительная открытая информация о них публикуется на общедоступном сервере. Полученная каждым участником секретная ключевая информация должна быть достаточной для вычисления каждым из них рабочих ключей для связи с участниками той или иной группы из числа групп, в которые он входит, и состав пакетов секретной информации которых ему известен. Состав самих групп также общеизвестен и публикуется. Они называются привилегированными. С другой стороны, имеются так называемые отчужденные группы участников. В правильно построенной схеме участники такой группы на основе объединения полученных каждым из ее участников пакетов секретной информации не должны вычислить рабочий ключ привилегированной группы. Это гарантируется условием корректности схемы.

Схемы предварительного распределения ключей с хешированием

Представим краткое описание свойств схем предварительного распределения ключей с хешированием, подробное описание которых можно найти в [2, 3].

Рассмотрим схему предварительного распределения q системных ключей с хешированием HAKDP($\boldsymbol{P}$, $\boldsymbol{F}$, L)(n,q) (Hashed Key Distribution Pattern) в компьютерной сети из n абонентов, в которых допускаются коалиции F участников из множества $\mathbf{F}$ отчужденных коалиций и группы P участников из множества $\mathbf{P}$ привилегированных групп участников. Интерпретируемы такие коалиции и группы как множества номеров входящих в них абонентов сети — подмножества множества $U = \{1, 2, ..., n\}$. Для получения этой схемы из исходного множества $\mathbf{K}$, $|\mathbf{K}| = q$, системных ключей (двоичных наборов фиксированной длины) образуется n подмножеств K_i, $i = 1, ..., n$ системных ключей, назначаемых i-му участнику. Для каждого участника определяется и публикуется на сервере пара числовых наборов (S_i, D_i). Наборы S_i содержат номера системных ключей из подмножеств K_i, а D_i — числа $D_i(s)$, $0 \le D_i \le L$, применений к этим ключам криптографической бесключевой хеш-функции $h:\{0,1\}^k \rightarrow \{0,1\}^k$. Получаемые в результате многократного применения к системному ключу хеш-функции образы системных ключей передаются i-му участнику по закрытому каналу.

Для вычисления общего ключа привилегированной группы P каждый ее участник (i-й абонент сети) должен применить функцию хеширования к полученному образу s системного ключа $\max_{j\in P} D_j(s) - D_i(s)$ раз.

Рабочий ключ, вычисляемый каждым участником группы P по образам системных ключей с номерами из множества $\bigcap_{i\in P} S_i$, имеющимися у каждого такого участника, не должен определяться участниками отчужденной группы на основе объединения полученных ими образов системных ключей, т. е. по образам ключей из множества $\bigcup_{i\in F} S_i$. Тогда при применении криптографической хеш-функции участники никакой отчужденной коалиции не смогут вычислить общий ключ участников привилегированной группы.

Изучаемые в работе HAKDP($\boldsymbol{P}$, $\boldsymbol{F}$, L)(n,q)-схемы, с одной стороны, являются обобщением KDP($\boldsymbol{P}$, $\boldsymbol{F}$)(n,q)-схем (Key Distribution Pattern) [1, 4 — 7], в которых не применяется хеширование и которые описываются наборами множеств S_i номеров системных ключей. Такие схемы впервые описаны в [6], где названы системами пересекающихся множеств (Set Intersection Systems). С другой стороны, они являются специальным подклассом так называемых HARPS(n,q)-схем (Hashed Random Preloaded Subset Key Distribution) [8], в которых каждому участнику доставляются все системные ключи из множества $\mathbf{K}$ $(\forall i \in P \bigcup F : S_i = \{1,...,q\})$.

Преимуществом KDP($\boldsymbol{P}$, $\boldsymbol{F}$)(n,q)-схем и их частного варианта KDP(n,q)-схем (множество $\mathbf{P}$ включает в себя все двухэлементные подмножества P, а множество $\mathbf{F}$ — все одноэлементные подмножества F) является их безусловная секретность, в то время как HAKDP($\boldsymbol{P}$, $\boldsymbol{F}$, L)(n,q)-схемы и HARPS(n,q)-схемы связаны с ограничением вычислительных возможностей участников сети, поскольку в них используются хеш-функции. Понятие HAKDP($\boldsymbol{P}$, $\boldsymbol{F}$, L)(n,q)-схем введено в [9].

Неформальное пояснение понятия HAKDP($\boldsymbol{P}$, $\boldsymbol{F}$, L)(n,q)-схемы формализуем следующим определением [2].

HAKDP($\boldsymbol{P}$, $\boldsymbol{F}$, L)(n,q)-схемой, где $\boldsymbol{P}$, $\boldsymbol{F}$ — семейства подмножеств множества $U = \{1, \ldots, n\}$, называется пара ($\tilde{\mathbf{K}}$, **D**) семейств $\tilde{\mathbf{K}} = \{K_1, \ldots, K_n\}$ подмножеств конечного множества **K** из q элементов (системных ключей) и $\mathbf{D} = \{D_1, \ldots, K_n\}$ подмножеств множества $\{0, 1, \ldots, L\}$, причем $|D_i| = |K_i|$ и элементы множеств D_i взаимно однозначно соответствуют элементам множеств K_i, $i = 1, \ldots, n$, удовлетворяющих условию предиката

$$\forall P \in \mathbf{P}, F \in \mathbf{F}, P \bigcap F = \varnothing : \bigcap_{i\in P} S_i \neq \neq \varnothing \wedge \{[\bigcap_{i\in P} S_i \not\subseteq \cup_{j\in F} S_j] \vee [\exists s \in \bigcap_{j\in P} S_j : : \max_{j\in P} D_j(s) < \min_{i\in F} D_i(s)]\}, \quad (1)$$

где S_i (или S_j) — множество номеров элементов множества **K**, образующих множество K_i (или K_j).

Представленные в (1) условия корректности схемы

$$\bigcap_{i\in P} S_i \not\subseteq \cup_{j\in F} S_j; \quad (2)$$

$$\exists s \in \bigcap_{j\in P} S_j : \max_{j\in P} D_j(s) < \min_{i\in F} D_i(s) \quad (3)$$

являются взаимно дополняющими. Для корректности схемы (соответствия предикату (1)) достаточно выполнение хотя бы одного их них. Называть (2) — KDP-, а (3) — HA-условиями.

Уравнениями (2), (3) обусловливается возможность сокращения как числа q распределяемых системных ключей, так и количества системных ключей, пересылаемых от доверенного центра участникам сети по защищенным каналам, т. е. повышения информационной скорости системы предварительного распределения ключей.

Об оценках объемов распределяемой ключевой информации для успешного синтеза схемы предварительного распределения ключей с хешированием с помощью вероятностного алгоритма

В работах [9, 10] обоснованы преимущества вероятностного алгоритма над детерминированными, а именно возможность существенного сокращения количества системных ключей. В [2] приведен расчет числа ключей q, достаточного для удачного синтеза схемы.

Опишем метод расчета минимального числа ключей $q_{\min}$, при котором может быть построена схема. Такое число практически недостижимо при экспериментах по синтезу схемы, тем не менее, оно объясняет возможность построения схемы с меньшим объемом распределяемой ключевой информации относительно достаточной оценки, а также позволит изучить информационную скорость схемы в идеальных условиях и найти максимальное ее значение.

Представим расчет достаточной оценки, приведенный в [2].

По определению паре ($\tilde{\mathbf{K}}$, **D**) взаимно однозначно соответствует пара семейств (**S**, **D**), где $\mathbf{S} = \{S_1, \ldots, S_n\}$. Вероятностный метод синтеза HAKDP(**P**, **F**, L)(n,q)-схемы заключается в случайном выборе пары семейств (**S**, **D**), при этом номера s включаются в множества S_i с вероятностью p, а $D_i(s)$ в множества D_i с вероятностью $1/(L + 1)$, и последующей проверке ее соответствия условию (1).

Если мощности элементов множества **P** равны g, а **F** — w, то HAKDP($\boldsymbol{P}$, $\boldsymbol{F}$, L)(n,k)-схему обозначим как HAKDP(g, w, L)(n,k).

Пусть **P** — семейство всех подмножеств множества **U** мощности g, **F** — семейство всех подмножеств множества **U** мощности w, причем $g + w \le n$.

Оценим вероятность $P_{L,g,w}$ того, что неравенство

$$\max_{i\in P} D_i(s) < \min_{i\in F} D_i(s)$$

в условии предиката (1) выполняется для всех $s \in \bigcap_{i\in P} S_i$.

Вероятность $P_{L,g,w}$ того, что эти события случаются при некотором t и указанное конкретное значение $D_{i\in F}(s)$ минимально (так как наборов $D_{i\in F}$ всего w штук), не меньше, чем

$$P'_{L,g,w} = \sum_{i=0}^{L} w^{-1} \frac{1}{L+1}\left(\frac{L-t}{L+1}\right)^g.$$

Математическое ожидание числа пар X множеств (**P**, **F**), для которых нарушено неравенство $\max_{j\in P} D_j(s) < \min_{i\in F} D_i(s)$ в условии предиката (1) для каждого s

$$E'[X](q,p,g,w) = \sum_{P\in\mathbf{P}} \sum_{\substack{F\in\mathbf{F} \\ P\bigcap F=\varnothing}} (1-p^g(1-p)^w - p^g(1-(1-p)^w)P'^{\,q}_{l,g,w}) = C_n^g C_{n-g}^w (1-p^g(1-p)^w - p^g(1-(1-p)^w)P'^{\,q}_{l,g,w}). \quad (4)$$

В $(1-p^g(1-p)^w) - p^g(1-p)^w)P'_{L,g,w}$ есть вероятность коллизии, т. е. нарушения указанного неравенства для конкретной пары множеств (**P**, **F**).

Число q ключей, получаемое логарифмированием неравенства

$$E'(q, p, g, w) < (1 - E) \quad (5)$$

при $E \to 1$, является достаточным для удачного синтеза схемы [2]:

$$q < \frac{\log\left(\dfrac{1-E}{C_n^g C_{n-g}^w}\right)}{\log\left(1-p^g((1-p)^w + p^w P_{L,g,w})\right)} = \frac{\log\left((1-E)\dfrac{g!w!}{(n-g-w+1)\ldots n}\right)}{\log\left(1-\left(p^g((1-p)^w + p^w P_{L,g,w})\right)\right)}. \quad (6)$$

Главное отличие в расчете минимальной оценки заключается в уходе от выполнения жесткого требования условия, когда указанное конкретное значение $D_{i\in F}(s)$

минимально, поскольку таких наборов — w штук. При этом несколько абонентов отчужденной группы могут обладать минимальным значением $D_{i\in F}$, а абоненты привилегированной группы, в свою очередь, максимальным значением $D_{i\in P}$, при этом неравенство $\max\limits_{i\in P} D_i(s) < \min\limits_{i\in F} D_i(s)$ в условии предиката (1) по-прежнему выполняется.

Приведем расчет оценки минимального распределяемого объема ключевой информации для схемы предварительного распределения ключей с взаимно дополняющими условиями их корректности.

Обозначим число $q_{\min}$ ключей как минимальное, при котором схема предварительного распределения с взаимно дополняющими условиями может быть синтезирована вероятностным алгоритмом, за неограниченное число итераций, т. е. $\lfloor q_{\min} - 1 \rfloor$ — это максимальное число ключей, при котором распределяемого ключевого материала не будет достаточно для синтеза схемы за сколь угодно много итераций вероятностного алгоритма.

Оценим вероятность $P_{L,g,w}$ того, что неравенство $\max\limits_{i\in P} D_i(s) < \min\limits_{i\in F} D_i(s)$ выполняется для всех $s \in \bigcap\limits_{i\in P} S_i$.

Рассчитаем вероятность, что выбранное значение $D_{i\in P}(s)$ больше всех остальных в наборе, следовательно, вероятность данного события равна g^{-1}.

Вероятность $P_{L,g,w}$ того, что эти события случаются при некотором i (указанное конкретное значение $D_{i\in F}(s)$ минимально, поскольку таких наборов w штук и значение $D_{i\in P}(s) < D_{i\in F}(s)$) определяется как

$$P'_{L,g,w} = \sum_{i=0}^{L} w^{-1} g^{-1}\left(\frac{L-t}{L+1}\right).$$

Таким образом, при расчете минимально возможного значения $q_{\min}$ исключаются строгие условия выполнения неравенств и выбирается наиболее благоприятный случай для синтеза схемы предварительного распределения ключей с взаимно дополняющими условиями, когда вычисляется простая вероятность выполнения этих условий.

Дальнейшие расчеты значения q_0 проводятся аналогично с учетом вероятности синтеза схемы $E = 0$ за одну итерацию вероятностного алгоритма.

Рассмотрим результаты расчета оценок и компьютерных экспериментов для серии схем HAKDP(3, w, 20) (16, q), w = 2, 3, 4 и при варьируемых параметрах p вероятностного алгоритма.

При p = 1 схемы серии соответствуют условию корректности (3), при p < 1 — условиям корректности (2) или (3), т. е. по совокупности — условию предиката (1).

В табл. 1 представлены значения q, полученные по (6), значения q', при которых удалось синтезировать корректную схему за t < 100 с, $q_{\min}$, при котором схема предварительного распределения ключей с взаимно дополняющими условиями может быть синтезирована вероятностным алгоритмом за неограниченное число итераций.

Таблица 1

Таблица значений объема распределяемой ключевой информации

p	w								
	2			3			4		
	q	$q_{\min}$	q'	q	$q_{\min}$	q'	q	$q_{\min}$	q'
0,5	466	58	145	603	88	290	1194	124	500
0,6	380	33	110	534	51	230	1142	73	450
0,7	255	21	94	497	32	210	1041	47	430
0,8	180	14	80	441	22-	205	835	32	410
0,9	130	10	76	351	15	205	613	23	410
0,95	112	9	75	303	13	205	522	20	410
0,99	99	8	75	268	12	205	461	17	410
1	96	8	75	260	11	205	447	17	410

В [2, 3] представлена серия схем, удовлетворяющая условию корректности (2). Схемы предварительного распределения ключей, удовлетворяющие только условию (2), сильно уступают по объему распределяемой ключевой информации как схемам, удовлетворяющим условию (3), так и схемам с взаимно дополняющими условиями.

Очевидно, минимальное значение количества единиц распределяемой ключевой информации значительно меньше как достаточной оценки, так и значения, достигнутого в ходе экспериментов по синтезу схем. Отсюда можно сделать вывод, что следует придерживаться достаточной оценки при выборе параметров схемы. Стоит отметить, что с ростом параметра p при увеличении размера привилегированных и отчужденных групп становится труднее достичь меньших значений параметра q. Таким образом, с ростом схемы и групп абонентов появляется проблема возрастающего объема необходимых вычислений для синтеза новой схемы. Условие корректности (2), соответствующее схеме KDP(**P**,**F**) позволяет сократить объем вычислений, что, в свою очередь, представляет большую практическую ценность при синтезе схемы.

Информационная скорость схем предварительного распределения ключей

В [1] D.R. Stinson вводит понятие информационной скорости схемы. Оно описывает эффективность, которая напрямую зависит от объема пересылаемой закрытой информации по защищенному каналу от доверенного центра участникам сети. Минимизация объема приводит к меньшей вероятности ошибки при пересылке и меньшей вычислительной нагрузке абонентов сети.

Для схем предварительного распределения ключей информационная скорость определяется как обратное к объему распределяемой ключевой информации:

Таблица 2

Значения параметров информационной скорости HAKDP(P, F, 20)(16, *q*)-схем предварительного распределения ключей

p	*w*								
	2			3			4		
	ρ	ρ_{max}	ρ′	ρ	ρ_{max}	ρ′	ρ	ρ_{max}	ρ′
0,5	0,268	2,155	0,862	0,207	1,420	0,431	0,105	1,008	0,250
0,6	0,274	3,157	0,947	0,195	2,042	0,453	0,091	1,427	0,231
0,7	0,350	4,252	0,950	0,180	2,790	0,425	0,086	1,900	0,208
0,8	0,434	5,580	0,977	0,177	3,551	0,381	0,094	2,441	0,191
0,9	0,534	6,944	0,914	0,198	4,630	0,339	0,113	3,019	0,169
0,95	0,587	7,310	0,877	0,217	5,061	0,321	0,126	3,289	0,160
0,99	0,638	7,891	0,842	0,236	5,261	0,308	0,137	3,714	0,154
1	0,651	7,813	0,833	0,240	5,208	0,305	0,140	3,676	0,152

$$\rho = \frac{1}{k_p};\ k_p = \sum_{\{i:P\in \mathrm{P}\}} s_i.$$

В табл. 2 представлен расчет значений информационной скорости для схем предварительного распределения ключей с взаимно дополняющими условиями их корректности. Каждое из значений умножено на 10^{-3}; для q_{min} значение информационной скорости составит ρ_{max} в силу обратной зависимости.

Как следует из табл. 2, максимальное значение информационной скорости схемы ожидаемо и достигается в столбце минимальных значений q_{min}. В рассчитываемых оценках, как в достаточной, так и в нижней, максимальное значение информационной скорости получается в случае $p = 1$, когда синтезированная схема соответствует HARPS(n,q)-схеме, что подтверждает влияние условия, соответствующего KDP(**P**, **F**)-схеме.

На практике требования к объему вычислений при синтезе схемы возрастают: чем больше объем привилегированных и отчужденных групп, тем дольше синтезируется схема. Таким образом, в больших схемах возрастает положительное влияние условия корректности (2), соответствующее схеме KDP(**P**, **F**), в силу чего следует выбирать меньшие значения параметра p. Также очевидно, что синтез схемы со значением $q' < q$ дает положительный результат относительно эффективности схемы (максимальные значения информационной скорости в соответствующих столбцах табл. 2), тем не менее, при выборе данного параметра следует выбирать значение, близкое к q', а не к q_{min}.

Исследование значений информационной скорости и эффективности схемы предварительного распределения ключей позволило обосновать преимущества HAKDP(**P**, **F**, L)(n,q)-схем предварительного распределения ключей с взаимно дополняющими условиями их корректности над частными случаями данной схемы. Кроме того, появилась возможность уточнить эффективные входные параметры, выбираемые для вероятностного алгоритма синтеза схемы.

Работа выполнена при поддержке РФФИ (проект № 17-01-00485а).

Литература

1. **Stinson D.R**. On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption // Designs Codes and Cryptography. 1997. V. 12. P. 215243.

2. **Фролов А.Б., Затей А.В.** Схемы предварительного распределения ключей с хешированием, допускающие коалиции // Вестник МЭИ. 2013. № 6. С. 166—172.

3. **Frolov A., Zatey A**. Probabilistic Synthesis of KDP Satisfying Mutually Complementary Correctness Conditions // Proc. Intern. Conf. Advances in Computing. Birmingham (UK), 2014.

4. **Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.** Основы криптографии. М: Гелиос АРВ, 2005.

5. **Dyer M., Fenner T., Frieze A., Thomason A.** On Key Storage in Secure Networks // J. Cryptology. 1995. V. 8. No. 4.Pp. 189—200.

6. **Щуров И.И.** Минимизация ключевого материала для построения безопасной сети // Вестник МЭИ. 2006. № 6. С. 112—118.

7. **Mitchell C.J., Piper F.C.** Key Storage in Secure Networks // Discrete Appl. Math. 1998. V. 21. Pp. 215—228.

8. **Ramkumar M., Memon N.** An Efficient Key Predistribution Scheme for ad Hoc Network Security. Selected Areas in Communications // IEEE J. Selected Areasin Communications. 2005. V. 23. No. 3. Pp. 611—621.

9. **Frolov A., Shchurov I.** Non-centralized Key Pre-Distribution in Computer Networks // Proc. of Intern. Conf. Dependability of computer Systems. Szklarska Poreba (Poland), 2008. Pp. 179—188.

10. **Фролов А.Б., Щуров И.И.** Защищенные коммуникации при нецентрализованном предварительном распределении ключей // Вестник МЭИ. 2008. № 4. С. 102—110.

References

1. **Stinson D.R**. On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption. Designs Codes and Cryptography. 1997;12:215243.

2. **Frolov A.B., Zatey A.V.** Skhemy Predvaritel'nogo Raspredeleniya Klyuchey s Heshirovaniem, Dopuskayushchie Koalitsii. Vestnik MPEI. 2013;6:166—172. (in Russian).

3. **Frolov A., Zatey A**. Probabilistic Synthesis of KDP Satisfying Mutually Complementary Correctness Conditions. Proc. Intern. Conf. Advances in Computing. Birmingham (UK), 2014.

4. **Alferov A.P., Zubov A.Yu., Kuz'min A.S., Cheremushkin A.V.** Osnovy Kriptografii. M: Gelios ARV, 2005. (in Russian).

5. **Dyer M., Fenner T., Frieze A., Thomason A.** On Key Storage in Secure Networks. J. Cryptology. 1995;8;4:189—200.

6. **Shchurov I.I**. Minimizatsiya Klyuchevogo Materiala dlya Postroeniya Bezopasnoy Seti. Vestnik MPEI. 2006;6:112—118. (in Russian).

7. **Mitchell C.J., Piper F.C.** Key Storage in Secure Networks. Discrete Appl. Math. 1998;21:215—228.

8. **Ramkumar M., Memon N.** An Efficient Key Predistribution Scheme for ad Hoc Network Security. Selected Areas in Communications. IEEE J. Selected Areasin Communications. 2005;23;3:611—621.

9. **Frolov A., Shchurov I.** Non-centralized Key Pre-Distribution in Computer Networks. Proc. of Intern. Conf. Dependability of computer Systems. Szklarska Poreba (Poland), 2008:179—188.

10. **Frolov A.B., Shchurov I.I.** Zashchishchennye Kommunikatsii pri Netsentralizovannom Predvaritel'nom Raspredelenii Klyuchey. Vestnik MPEI. 2008;4:102—110. (in Russian).

Сведения об авторе

Затей Александр Васильевич — студент НИУ «МЭИ», e-mail: theseus_91@mail.ru

Information about author

Zatey Aleksandr V. — student, NRU MPEI, e-mail: theseus_91@mail.ru

Статья поступила в редакцию 28.03.2017