УДК 519.72

О ПОСТРОЕНИИ СОВЕРШЕННЫХ ШИФРОВ

С. М. Рацеев

Ульяновский государственный университет,
Россия, 432017, Ульяновск, ул. Л. Толстого, 42.

К. Шеннон в 40-х годах XX века ввел понятие совершенного шифра, обеспечивающего наилучшую защиту открытых текстов. Такой шифр не дает криптоаналитику никакой дополнительной информации об открытом тексте на основе перехваченной криптограммы. В работе исследуется задача построения совершенных шифров по заданному множеству открытых текстов X, ключей K и распределению вероятностей $P(K)$ на множестве ключей. Приводится критерий, позволяющий однозначно определить, существует ли для заданных X, K, $P(K)$ совершенный шифр. Показано, что данная задача сводится к построению набора разбиений множества K с определёнными условиями. Так как одним из недостатков вероятностной модели шифра являются ограничения, накладываемые на мощности множеств открытых текстов, ключей и шифрованных текстов, в работе также рассматривается задача построения совершенного шифра замены с неограниченным ключом по заданному множеству шифрвеличин, ключей и распределению вероятностей на множестве ключей.

Ключевые слова: *шифр, совершенный шифр, набор ключей, распределение вероятностей.*

Пусть X, K, Y — конечные множества открытых текстов, ключей и шифрованных текстов соответственно. Обозначим через

$$\Sigma_B = (X, K, Y, E, D, P(X), P(K))$$

вероятностную модель шифра (см. [1]), где E и D — множества правил зашифрования и расшифрования соответственно. При этом предполагается, что априорные распределения вероятностей $P(X)$ и $P(K)$ на соответствующих множествах X и K независимы и не содержат нулевых вероятностей. Распределения $P(X)$ и $P(K)$ естественным образом индуцируют распределение вероятностей $P(Y)$ следующим образом:

$$P_Y(y) = \sum_{\substack{(x,k)\in X\times K \\ E_k(x)=y}} P_X(x)\cdot P_K(k).$$

Обозначим через $K(x, y)$ множество всех таких ключей $k \in K$, для которых $E_k(x) = y$. Условная вероятность $P_{Y|X}(y|x)$ определяется естественным образом:

$$P_{Y|X}(y|x) = \begin{cases} \sum_{k\in K(x,y)} P_K(k), & K(x,y) \neq \emptyset, \\ 0, & K(x,y) = \emptyset. \end{cases}$$

ISSN: 2310-7081 (online), 1991-8615 (print); doi: http://dx.doi.org/10.14498/vsgtu1271

Образец цитирования: С. М. Рацеев, “О построении совершенных шифров” // *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2014. № 1 (34). С. 192–199. doi: 10.14498/vsgtu1271.

Сведения об авторе: *Сергей Михайлович Рацеев* (к.ф.-м.н.), доцент, каф. информационной безопасности и теории управления.

E-mail address: RatseevSM@mail.ru

С помощью теоремы умножения вероятностей можно определить и условную вероятность $P_{Y|X}(y|x)$:

$$P_{X|Y}(x|y) = \frac{P_X(x) \cdot P_{Y|X}(y|x)}{P_Y(y)}.$$

Напомним, что шифр Σ_B называется совершенным по Шеннону [2], если для любых $x \in X$, $y \in Y$ выполнено равенство $P_{X|Y}(x|y) = P_X(x)$. Приведем эквивалентные, необходимые и достаточные условия совершенного по Шеннону шифра.

Предложение 1. *Для произвольного шифра Σ_B следующие условия эквивалентны*:

(i) *для любых $x \in X$, $y \in Y$ выполнено равенство $P_{X|Y}(x|y) = P_X(x)$*;
(ii) *для любых $x \in X$, $y \in Y$ выполнено равенство $P_{Y|X}(y|x) = P_Y(y)$*;
(iii) *для любых $x_1, x_2 \in X$, $y \in Y$ выполнено равенство $P_{Y|X}(y|x_1) = P_{Y|X}(y|x_2)$*.

Предложение 2 [1]. *Пусть Σ_B — совершенный по Шеннону шифр. Тогда для шифра Σ_B будут выполнены следующие условия*:

(i) *для любых $x \in X$, $y \in Y$ найдётся такой ключ $k \in K$, что $E_k(x) = y$*;
(ii) *для множеств X, Y и K справедливо двойное неравенство $|X| \leqslant |Y| \leqslant |K|$*.

Теорема 1 [3] (достаточные условия совершенного по Шеннону шифра). *Пусть для шифра Σ_B выполнены следующие условия*:

(i) *$|K(x, y)| = 1$ для любых $x \in X$, $y \in Y$*;
(ii) *распределение вероятностей $P(K)$ является равномерным.*

Тогда шифр Σ_B является совершенным по Шеннону, причём распределение вероятностей $P(Y)$ будет являться равномерным и $|K| = |Y|$.

Следствие (теорема К. Шеннона). *Пусть Σ_B — некоторый шифр, для которого выполнено равенство $|X| = |K| = |Y|$. Шифр Σ_B является совершенным по Шеннону тогда и только тогда, когда выполнены следующие условия*:

(i) *$|K(x, y)| = 1$ для любых $x \in X$, $y \in Y$*;
(ii) *распределение вероятностей $P(K)$ является равномерным.*

Рассмотрим следующую задачу: по заданному множеству открытых текстов X_0 и множеству ключей K_0 с распределением вероятностей $P(K_0)$ (независимо от $P(X_0)$) однозначно определить, существует ли шифр

$$\Sigma_B = (X_0, K_0, Y, E, D, P(X_0), P(K_0)),$$

являющийся совершенным по Шеннону.

Теорема 2. *Для заданных X, $|X| = n$, K, $|K| = m$, $P(K)$ существует совершенный шифр*

$$\Sigma_B = (X, K, Y, E, D, P(X), P(K))$$

тогда и только тогда, когда выполнены следующие условия:

1) *существует* n *разбиений множества* K, *которые состоят из одинакового количества непустых частей*:

$$K = K_{11} \cup K_{12} \cup \cdots \cup K_{1s}, \quad K_{1i} \cap K_{1j} = \emptyset, \quad 1 \leqslant i < j \leqslant s,$$

$$K = K_{21} \cup K_{22} \cup \cdots \cup K_{2s}, \quad K_{2i} \cap K_{2j} = \emptyset, \quad 1 \leqslant i < j \leqslant s,$$

$$\cdots$$

$$K = K_{n1} \cup K_{n2} \cup \cdots \cup K_{ns}, \quad K_{ni} \cap K_{nj} = \emptyset, \quad 1 \leqslant i < j \leqslant s;$$

2) $K_{it} \cap K_{jt} = \emptyset$, $1 \leqslant i < j \leqslant n$, $t = 1, \ldots, s$;
3) *для любых* $1 \leqslant i < j \leqslant n$, $t = 1, \ldots, s$ *выполнено равенство*

$$\sum_{k \in K_{it}} P_K(k) = \sum_{k \in K_{jt}} P_K(k).$$

Доказательство. Достаточность. Пусть для X, K, $P(K)$ выполнены условия 1)–3). Пусть $Y = \{y_1, \ldots, y_s\}$ — некоторое множество шифрованных текстов, где s — число непустых частей из условия 1). Составим матрицу зашифрования размера $m \times n$, где строки пронумерованы элементами множества K, а столбцы — элементами множества X, следующим образом. В i-том столбце ($i = 1, \ldots, n$) данной матрицы в строках, пронумерованных элементами множества K_{ij}, поставим элемент y_j, $j = 1, \ldots, s$. Условие 2) в этом случае гарантирует, что все правила зашифрования полученного шифра являются инъективными отображениями. А из условия 3) следует, что для любого $t = 1, \ldots, s$ и любых $1 \leqslant i < j \leqslant n$ будут выполнены равенства

$$P_{Y|X}(y_t|x_i) = \sum_{k \in K_{it}} P_K(k) = \sum_{k \in K_{jt}} P_K(k) = P_{Y|X}(y_t|x_j).$$

Поэтому, учитывая предложение 1, полученный шифр будет являться совершенным по Шеннону.

Необходимость. Пусть для заданных X, K, $P(K)$ существует совершенный по Шеннону шифр Σ_B со множеством шифртекстов $Y = \{y_1, \ldots, y_s\}$. Обозначим для данного шифра

$$K_{it} = \{k \in K \mid E_k(x_i) = y_t\}, \quad i = 1, \ldots, n, \quad t = 1, \ldots, s.$$

Понятно, что

$$P_{Y|X}(y_t|x_i) = \sum_{k \in K_{it}} P_K(k).$$

Из предложений 1 и 2 следует, что для множеств K_{it} будут выполнены условия 1)–3). □

Пример. Пусть $X = \{x_1, x_2\}$, $K = \{k_1, k_2, k_3, k_4\}$ и распределение вероятностей на множестве K имеет вид

K	k_1	k_2	k_3	k_4
$P(K)$	1/8	1/4	3/8	1/4

В этом случае можно построить два разбиения множества K вида

$$K = \{k_1, k_2\} \cup \{k_3\} \cup \{k_4\},$$

$$K = \{k_3\} \cup \{k_1, k_4\} \cup \{k_2\},$$

где

$$\{k_1, k_2\} \cap \{k_3\} = \{k_3\} \cap \{k_1, k_4\} = \{k_4\} \cap \{k_2\} = \emptyset.$$

При этом будут выполнены равенства

$$P_K(k_1) + P_K(k_2) = P_K(k_3),$$

$$P_K(k_3) = P_K(k_1) + P_K(k_4),$$

$$P_K(k_4) = P_K(k_2).$$

По теореме 2 для данных X, K, $P(K)$ можно построить совершенный шифр. Пусть $Y = \{y_1, y_2, y_3\}$. Составим матрицу зашифрования следующим образом:

$K \diagdown X$	x_1	x_2
k_1	y_1	y_2
k_2	y_1	y_3
k_3	y_2	y_1
k_4	y_3	y_2

Тогда полученный шифр будет являться совершенным по Шеннону.

Определенная вероятностная модель шифра Σ_B позволяет рассматривать в качестве множества открытых текстов X лишь последовательности в некотором конечном алфавите A, длины которых ограничены некоторой заранее определенной константой. В работе [4] приводятся модели шифров замены с ограниченным и неограниченным ключом, для которых, в частности, на множество X такое ограничение не накладывается. Поскольку в общем случае шифр замены с ограниченным ключом совершенным не является (см. [4]), нас будет интересовать шифр замены с неограниченным ключом. Такая математическая модель имеет ряд полезных свойств, например, она позволяет строить модели совершенных шифров и оптимальных кодов аутентификации, стойких к имитации и подмене [3, 5].

Приведем модель данного шифра.

Пусть U — конечное множество возможных «шифрвеличин», а V — конечное множество возможных «шифробозначений». Пусть также имеются r ($r > 1$) инъективных отображений из U в V. Пронумеруем данные отображения: E_1, E_2, …, E_r. Данные отображения называются простыми заменами. Обозначим $\mathbb{N}_r = \{1, 2, \ldots, r\}$. Опорным шифром замены назовём совокупность $\Sigma = (U, \mathbb{N}_r, V, E, D)$, для которой выполнены следующие свойства:

1) для любых $u \in U$ и $j \in \mathbb{N}_r$ выполнено равенство $D_j(E_j(u)) = u$;
2) $V = \bigcup_{j \in \mathbb{N}_r} E_j(U)$.

При этом $E = \{E_1, \ldots, E_r\}$, $D = \{D_1, \ldots, D_r\}$, $D_j : E_j(U) \to U$, $j \in \mathbb{N}_r$.

l-той степенью опорного шифра Σ назовём совокупность

$$\Sigma^l = (U^l, \mathbb{N}_r^l, V^l, E^{(l)}, D^{(l)}),$$

где $U^l, \mathbb{N}_r^l, V^l$ — декартовы степени соответствующих множеств $U, \mathbb{N}_r, V$. Множество $E^{(l)}$ состоит из отображений $E_{\overline{j}} : U^l \to V^l$, $\overline{j} \in \mathbb{N}_r^l$ таких, что для любых $\overline{u} = u_1 \dots u_l \in U^l$, $\overline{j} = j_1 \dots j_l \in \mathbb{N}_r^l$ выполнено равенство

$$E_{\overline{j}}(\overline{u}) = E_{j_1}(u_1) \dots E_{j_l}(u_l) = v_1 \dots v_l \in V^l,$$

а множество $D^{(l)}$ состоит из отображений $D_{\overline{j}} : E_{\overline{j}}(U^l) \to U^l$, $\overline{j} \in \mathbb{N}_r^l$, таких что для любых $\overline{v} = v_1 \dots v_l \in V^l$, $\overline{j} = j_1 \dots j_l \in \mathbb{N}_r^l$ выполнено равенство

$$D_{\overline{j}}(\overline{v}) = D_{j_1}(v_1) \dots D_{j_l}(v_l) = u_1 \dots u_l \in U^l.$$

Отметим важный момент. В ряде случаев не всякое слово длины l в алфавите U может появиться в открытом тексте. Поэтому обозначим через $U^{(l)}$ подмножество всех таких слов во множестве U^l, появление которых в открытом тексте имеет ненулевую вероятность:

$$U^{(l)} = \{\overline{u} \in U^l \mid P_{U^l}(\overline{u}) > 0\}.$$

Тогда

$$V^{(l)} = \bigcup_{\overline{j} \in \mathbb{N}_r^l} E_{\overline{j}}(U^{(l)}).$$

Пусть ψ_c — случайный генератор ключевого потока, который для любого натурального числа l вырабатывает случайный ключевой поток $j_1 \dots j_l$, где все $j_i \in \mathbb{N}_r$.

Обозначим через Σ_H^l следующую совокупность величин:

$$\Sigma_H^l = (U^{(l)}, \mathbb{N}_r^l, V^{(l)}, E^{(l)}, D^{(l)}, P(U^{(l)}), P(\mathbb{N}_r^l)).$$

Шифром замены с неограниченным ключом назовём семейство

$$\Sigma_H = (\Sigma_H^l,\ l \in \mathbb{N};\ \psi_c).$$

При этом независимые и не содержащие нулевых вероятностей распределения $P(U^{(l)})$ и $P(\mathbb{N}_r^l)$ индуцируют распределения вероятностей на множестве $V^{(l)}$:

$$P_{V^{(l)}}(\overline{v}) = \sum_{\substack{(\overline{u},\overline{j}) \in U^{(l)} \times \mathbb{N}_r^l \\ E_{\overline{j}}(\overline{u}) = \overline{v}}} P_{U^{(l)}}(\overline{u}) \cdot P_{\mathbb{N}_r^l}(\overline{j}).$$

Также определим условные вероятности $P_{U^{(l)}|V^{(l)}}(\overline{u}|\overline{v})$ и $P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{u})$:

$$P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{u}) = \sum_{\overline{j} \in \mathbb{N}_r^l(\overline{u},\overline{v})} P_{\mathbb{N}_r^l}(\overline{j}), \qquad P_{U^{(l)}|V^{(l)}}(\overline{u}|\overline{v}) = \frac{P_{U^{(l)}}(\overline{u}) \cdot P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{u})}{P_{V^{(l)}}(\overline{v})},$$

где $\mathbb{N}_r^l(\overline{u}, \overline{v}) = \{\overline{j} \in \mathbb{N}_r^l \mid E_{\overline{j}}(\overline{u}) = \overline{v}\}$.

Говорят, что шифр Σ_H является совершенным тогда и только тогда, когда для любого натурального l шифр Σ_H^l является совершенным по Шеннону.

Предложение 3. *Для шифра Σ_H следующие условия эквивалентны*:

(i) *для любого* $l \in \mathbb{N}$ *и любых* $\overline{u} \in U^{(l)}$, $\overline{v} \in V^{(l)}$ *выполнено равенство* $P_{U^{(l)}|V^{(l)}}(\overline{u}|\overline{v}) = P_{U^{(l)}}(\overline{u})$;

(ii) *для любого* $l \in \mathbb{N}$ *и любых* $\overline{u} \in U^{(l)}$, $\overline{v} \in V^{(l)}$ *выполнено равенство* $P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{u}) = P_{V^{(l)}}(\overline{v})$;

(iii) *для любого* $l \in \mathbb{N}$ *и любых* $\overline{u}_1, \overline{u}_2 \in U^{(l)}$, $\overline{v} \in V^{(l)}$ *выполнено равенство* $P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{u}_1) = P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{u}_2)$.

Теорема 3 [3] (достаточные условия совершенности шифра Σ_H). *Пусть шифр замены* Σ_H *обладает следующими условиями*:

(i) *правила зашифрования* $E_1, E_2, \ldots, E_r$ *шифра* Σ_H *обладают тем свойством, что для любых* $u \in U$, $v \in V$ *найдётся, и притом единственный, элемент* $j = j(u, v) \in \mathbb{N}_r$ *такой, что* $E_j(u) = v$;

(ii) *распределение вероятностей* $P(\mathbb{N}_r)$ *является равномерным.*

Тогда шифр Σ_H *является совершенным, причём для любого* $l \in \mathbb{N}$ *выполнено равенство* $|V^{(l)}| = r^l$ *и распределение вероятностей* $P(V^{(l)})$ *будет являться равномерным.*

Теорема 4 *Пусть для шифра* Σ_H *выполнено равенство* $|U| = |\mathbb{N}_r| = |V|$. *Шифр* Σ_H *является совершенным тогда и только тогда, когда выполнены следующие условия*:

(i) *правила зашифрования* $E_1, E_2, \ldots, E_r$ *шифра* Σ_H *обладают тем свойством, что для любых* $u \in U$, $v \in V$ *найдётся, и притом единственный, элемент* $j = j(u, v) \in \mathbb{N}_r$ *такой, что* $E_j(u) = v$;

(ii) *распределение вероятностей* $P(\mathbb{N}_r)$ *является равномерным.*

Доказательство следует из теоремы Шеннона и теоремы 3.

Рассмотрим задачу построения совершенного шифра Σ_H по заданному множеству «шифрвеличин» U и множеству $\mathbb{N}_r$ с распределением вероятностей $P(\mathbb{N}_r)$.

Теорема 5. *Для заданных* U, $|U| = n$, $\mathbb{N}_r$, $P(\mathbb{N}_r)$ *существует совершенный шифр* Σ_H *тогда и только тогда, когда выполнены следующие условия*:

1) *существует* n *разбиений множества* $\mathbb{N}_r$, *которые состоят из одинакового количества непустых частей*:

$$\mathbb{N}_r = K_{11} \cup K_{12} \cup \cdots \cup K_{1s}, \quad K_{1i} \cap K_{1j} = \emptyset, \quad 1 \leqslant i < j \leqslant s,$$

$$\mathbb{N}_r = K_{21} \cup K_{22} \cup \cdots \cup K_{2s}, \quad K_{2i} \cap K_{2j} = \emptyset, \quad 1 \leqslant i < j \leqslant s,$$

$$\ldots$$

$$\mathbb{N}_r = K_{n1} \cup K_{n2} \cup \cdots \cup K_{ns}, \quad K_{ni} \cap K_{nj} = \emptyset, \quad 1 \leqslant i < j \leqslant s;$$

2) $K_{it} \cap K_{jt} = \emptyset$, $1 \leqslant i < j \leqslant n$, $t = 1, \ldots, s$;

3) $\sum\limits_{k \in K_{it}} P_{\mathbb{N}_r}(k) = \sum\limits_{k \in K_{jt}} P_{\mathbb{N}_r}(k), \quad 1 \leqslant i < j \leqslant n, \quad t = 1, \ldots, s.$

Доказательство. Необходимое условие следует из теоремы 2.

Достаточность. Пусть выполнены условия 1)–3) и пусть V — некоторое множество «шифробозначений», $|V| = s$. Составим матрицу зашифрования

над элементами множества V для опорного шифра Σ так же, как и в теореме 2. Зафиксируем некоторое натуральное l. Пусть

$$\overline{a} = a_1 \dots a_l \in U^{(l)}, \quad \overline{b} = b_1 \dots b_l \in U^{(l)}, \quad \overline{v} = v_1 \dots v_l \in V^{(l)}.$$

Тогда

$$P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{a}) = \prod_{i=1}^{l} P_{V|U}(v_i|a_i) = \prod_{i=1}^{l} P_{V|U}(v_i|b_i) = P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{b}),$$

где второе равенство следует из теоремы 2. Поэтому из предложения 3 следует, что шифр Σ_H^l является совершенным по Шеннону. □

СПИСОК ЛИТЕРАТУРЫ/ REFERENCES

1. А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин, *Основы криптографии*, М.: Гелиос, АРВ, 2005. 480 с. [A. P. Alferov, A. Yu. Zubov, A. S. Kuz'min, A. V. Cheremushkin, *Osnovy kriptografii* [Foundations of Cryptography], Moscow, Helios, Association of Russian Universities, 2005, 480 pp. (In Russian)]
2. C. E. Shannon, "Communication Theory of Secrecy Systems", *Bell System Technical Journal*, 1949, vol. 28, no. 4, pp. 656–715. doi: 10.1002/j.1538-7305.1949.tb00928.x; К. Шеннон, "Теория связи в секретных системах" / *Работы по теории информации и кибернетике*, М.: Иностранная литература, 1963. С. 333–369.
3. С. М. Рацеев, "О совершенных имитостойких шифрах" // *ПДМ*, 2012. №3. С. 41–46. [S. M. Ratseev, "About perfect imitation resistant ciphers", *Prikl. Diskr. Mat.*, 2012, no. 3, pp. 41–46. (In Russian)].
4. А. Ю. Зубов, *Криптографические методы защиты информации. Совершенные шифры*, М.: Гелиос, АРВ, 2005. 192 с. [A. Yu. Zubov, *Kriptograficheskie metody zashchity informatsii. Sovershennye shifry* [Cryptographic methods of information protection. Perfect codes], Moscow, Helios, Association of Russian Universities, 2005, 192 pp. (In Russian)]
5. С. М. Рацеев, "Об оптимальных кодах аутентификации" // *Системы и средства информ.*, 2013. Т. 23, №1, «Проблемы информационной безопасности и надежности систем информатики». С. 53–57. [S. M. Ratseev, "On optimal authentication code", *Sistemy i Sredstva Inform.*, 2013, vol. 23, no. 1, pp. 53–57. (In Russian)].

Поступила в редакцию 22/X/2013;
в окончательном варианте — 27/I/2014;
принята в печать — 27/I/2014.

MSC: 68P25, 94A60

ON CONSTRUCTION OF PERFECT CIPHERS

S. M. Ratseev

Ulyanovsk State University,
42, L. Tolstoy st., Ulyanovsk, 432017, Russian Federation.

K. Shannon in the 40s of the 20th century introduced the concept of a perfect cipher, which provides the best protection of plaintexts. Perfect secrecy means that cryptanalyst can obtain no information about the plaintext by observing the ciphertext. In the paper we study the problem of construction of perfect ciphers on a given set of plaintexts X, a set of keys K and a probability distribution $P(K)$. We give necessary and sufficient conditions for a perfect ciphers on given X, K and $P(K)$. It is shown that this problem is reduced to construction of the set of partitions of the set K with certain conditions. As one of the drawbacks of the probability model of cipher are limitations on the power of sets of plaintexts, keys and ciphertexts we also study the problem of construction of substitution cipher with unbounded key on a given set of ciphervalues, a set of keys and a probability distribution on the set of keys.

Keywords: *cipher, perfect cipher, set of keys, probability distribution.*

Received 22/X/2013;
received in revised form 27/I/2014;
accepted 27/I/2014.

ISSN: 2310-7081 (online), 1991-8615 (print); doi: http://dx.doi.org/10.14498/vsgtu1271

Citation: S. M. Ratseev, "On Construction of Perfect Ciphers", *Vestn. Samar. Gos. Tekhn. Univ., Ser. Fiz.-Mat. Nauki* [J. Samara State Tech. Univ., Ser. Phys. & Math. Sci.], 2014, no. 1 (34), pp. 192–199. doi: 10.14498/vsgtu1271. (In Russian)
Author Details: *Sergey M. Ratseev* (Cand. Phys. & Math. Sci.), Associate Professor, Dept. of Information Security & Control Theory.

E-mail address: RatseevSM@mail.ru