УДК 512.6, 519.165, 519.725

О КОНСТРУКЦИЯХ ИДЕАЛЬНЫХ СОВЕРШЕННЫХ ПОЧТИ ПОРОГОВЫХ СХЕМ РАЗДЕЛЕНИЯ СЕКРЕТА

Медведев Н.В.[1], Титов С.С.[1]

[1]*ФГБОУ ВПО «Уральский государственный университет путей сообщения», г. Екатеринбург, Россия (620034, г. Екатеринбург, ул. Колмогорова, 66), e-mail: itcrypt@gmail.com*

В статье рассмотрены вопросы, связанные с информационной безопасностью, а именно, разделение секрета и делегирование прав участников. Обсуждается проблема реализации сложных структур доступа, в том числе с использованием эллиптических кривых. Поскольку идеальным схемам разделения секрета соответствуют матроиды, изучение которых дает структуру доступа, представлен двойственный вариант аксиоматизации матроидов с помощью антициклов, т.е. нуль-множеств. Через геометрическую интерпретацию представленных аксиом дан ряд конструкций почти пороговых схем разделения секрета и соответствующих им матроидов. Доказано, что реализуется бесконечная серия матроидов M на m-мерном проективном и аффинном пространстве над GF(q) с одинаковой мощностью циклов. Циклы матроида определяются как дополнения нуль-множеств. В качестве нуль-множеств берутся гиперпространства в M. Таким образом, построен бесконечный класс почти пороговых идеальных совершенных схем разделения секрета и их матроидов, при помощи комбинаторных методов конечных геометрий. Показана реализация идеальной совершенной почти пороговой схемы разделения секрета на эллиптической кривой, на которой многочлен третьей степени используется для генерации проверочной матрицы над GF(q) кода линейной схемы разделения секрета. Представлен пример реализации такой схемы при помощи эллиптических кривых над GF(3).

Ключевые слова: схемы разделения секрета, разграничение доступа, матроиды, эллиптические кривые.

ON CONSTRUCTURES OF IDEAL PERFECT ALMOST-THRESHOLD SECRET SHARING SCHEMES

Medvedev N.V.[1], Titov S.S.[1]

[1]*Ural State University of Railway Transport, Ekaterinburg, Russia (620034, Ekaterinburg, street Kolmogorov, 66), e-mail: itcrypt@gmail.com*

The article deals with issues related to information security, namely, of the secret sharing schemes and delegation rights of participants. The problem of implementing complex access structures is discuss, including the use of elliptic curves. As an ideal secret sharing scheme correspond to matroids, the study of access structure is presented as a dual version of the axiomatization of matroids with anticycles, i.e. zero-sets. By a geometric interpretation of these axioms is submitted with a number of designs of almost-threshold secret sharing schemes and their associated matroids. It is proved that an infinite series of realized matroids M on m-dimensional projective and affine space over GF(q) with the same power cycles. The cycles of the matroid defined as additions zero-sets. As the zero-sets are taken hyperspaces of M. Thus, an infinite class of almost-threshold ideal perfect secret sharing schemes and matroids is constructed, using combinatorial methods of finite geometries. The implementation of perfect ideal threshold secret sharing schemes are shown on an elliptic curve, on which third-degree polynomial is used to generate the check matrix of code over GF(q) as, a linear secret sharing schemes. An example of the implementation of this scheme with the help of elliptic curves over GF(3) is presented.

Keywords: secret sharing schemes, access control, matroids, elliptic curves.

Введение

Информационная безопасность является одной из составляющих национальной безопасности РФ и оказывает влияние на различные сферы жизнедеятельности общества и государства [3]. Поэтому вопросы, связанные с зашитой информации и с соответствующими математическими задачами, являются чрезвычайно важными. Такими, например, являются

задачи разграничения доступа к информации [4] и разделения секрета, в том числе со сложной структурой доступа.

Основная идея схемы разделения секрета (СРС) состоит [2,8] в раздаче *долей секрета* участникам таким образом, чтобы заранее заданные коалиции участников (разрешенные коалиции) могли однозначно восстановить секрет (совокупность этих множеств называется *структурой доступа*), а неразрешенные – не получали никакой дополнительной, к имеющейся априорной, информации о возможном значении секрета. Такие СРС называются *совершенными*. *Идеальными* называются СРС, где размер доли секрета, предоставляемый участнику, не больше самого размера секрета. Если разрешенными коалициями являются любые множества из n или более элементов, то такие СРС называются *пороговыми* «n из N» СРС, где N – количество всех участников. В работе [6] ранее были описаны СРС при помощи многочленов на эллиптических кривых, в которой минимальные разрешённые коалиции участников имели близкую мощность, т.е. либо n, либо $n+1$. Такие схемы были названы *почти пороговыми*. Разрешенные коалиции идеальной схемы разделения секрета определяются циклами некоторого связного *матроида* (см. далее), изучение которого и дает структуру доступа [2,8].

Цель данного исследования – построение классов почти пороговых идеальных совершенных схем разделения секрета и их матроидов, при помощи комбинаторных методов конечных геометрий.

Аксиоматизация матроидов

Как известно [1], на множестве H определен матроид, если некоторые его подмножества названы *независимыми* (остальные – *зависимыми*), причём удовлетворяются аксиомы матроида. Известно много вариантов аксиоматизации матроидов [1]. Например, в терминах *циклов*, т.е. минимальных по включению зависимых подмножеств из H, аксиом всего две. Представляется естественным рассмотреть двойственный вариант к аксиоматизации в терминах циклов, а именно, использовать не циклы C матроида M, а его нуль-множества Z, т.е. $Z = M \setminus C$, которые можно назвать «*антициклами*». Тогда аксиомы матроида в терминах антициклов имеют следующий вид: 1) нет антицикла в антицикле, т.е. если Z_1, Z_2 – антициклы, и $Z_1 \subset Z_2$, то $Z_1 = Z_2$; 2) если $e \in M$, $e \notin Z_1 \bigcup Z_2$ и Z_1, Z_2 – антициклы, причем $Z_1 \neq Z_2$, то существует такой антицикл Z, что $(\{e\} \bigcup (Z_1 \bigcap Z_2)) \subset Z$.

Напомним, что матроид называется *связным*, если для любых двух его элементов существует содержащий их цикл. Почти пороговым СРС соответствуют матроиды, которые было естественно назвать *почти пороговыми*, в том смысле, что его антициклы имеют близкую мощность.

Наша задача – через геометрическую интерпретацию представленных выше аксиом дать ряд конструкций почти пороговых СРС и соответствующих им матроидов.

Матроиды на проективном и аффинном пространстве

Пусть M – проективное m-мерное пространство над GF(q). Возьмем в качестве нуль-множеств Z гиперпространства в M. Как известно [7], $|M| = (q^{m+1}-1)/(q-1)$ и $|Z| = (q^m-1)/(q-1)$. Поскольку любые два гиперпространства Z_i и Z_j всегда пересекаются, т.е. $(Z_i \bigcap Z_j) \neq \varnothing$, причем размерность $\dim Z = m-1$, $\dim(Z_i \bigcap Z_j) = m-2$, то для любой точки $e \notin (Z_i \bigcap Z_j)$, существует единственное гиперпространство Z, натянутое на $\{e\}$ и на пересечение гиперпространств Z_i и Z_j, так что $Z = \langle \{e\}, Z_i \bigcap Z_j \rangle$. А это – не что иное, как вторая аксиома матроида в терминах антициклов, которую можно назвать усиленной, т.к. существует единственное такое гиперпространство. Следовательно, вторая аксиома матроида выполняется. Первая аксиома матроида с очевидностью выполняется, т.к. размерности гиперпространств одинаковы и антицикла в антицикле быть не может. Итак, доказано

Утверждение 1. Проективное пространство M является матроидом над GF(q) с гиперпространствами в качестве антициклов.

Поскольку все циклы матроида M определяются как дополнения нуль-множеств Z, размерность которых одинакова, то отсюда вытекает

Утверждение 2. Циклы матроида в m-мерном проективном пространстве M имеют одинаковую мощность $|C| = |M \setminus Z| = q^m$.

Перейдем к рассмотрению матроидов в аффинном m-мерном пространстве M над GF(q). Как известно, $|M| = q^m$ и $|Z| = q^{m-1}$. В аффинном пространстве может быть два случая пересечения гиперпространств Z_i и Z_j: 1) либо пересекаются, т.е. $Z_i \bigcap Z_j \neq \varnothing$, тогда вторая аксиома матроида выполняется, что было доказано выше, как в проективном пространстве; 2) либо параллельны, т.е. $Z_i \bigcap Z_j = \varnothing$, тогда это тривиальный случай и вторая аксиома матроида также выполняется, т.к. объединение двух соответствующих гиперпространствам циклов будет все пространство M. Первая аксиома матроида аналогично выполняется в обоих случаях как в проективном пространстве. Итак, доказано

Утверждение 3. Аффинное пространство M является матроидом над GF(q) с гиперпространствами в качестве антициклов.

Поскольку все циклы матроида M определяются как дополнения нуль-множеств Z, размерность которых одинакова, то отсюда вытекает

Утверждение 4. Циклы матроида в m-мерном аффинном пространстве M имеют одинаковую мощность $|C| = |M \setminus Z| = q^m - q^{m-1}$.

При реализации такой СРС гиперпространства соответствуют линейным функциям, т.е. функциями вида $f(x_1,...,x_m) = f_0 + f_1x_1 + ... + f_mx_m$, где $x_1,...,x_m \in GF(q) = F_q$ и $f_0, f_1,..., f_m \in GF(q)$. Позиции кода – точки $(x_1,...,x_m)$ m-мерного пространства F_q^m (они же – участники СРС), код состоит из тех q^m-мерных векторов, т.е. функций $s(x_1,...,x_m): F_q^m \to F_q$, что $\sum_{x_1,...,x_m} s(x_1,...,x_m) \cdot f(x_1,...,x_m) = 0$ для всех линейных непостоянных функций f.

Рассмотрим пример для q=3 и m=2. Построим табл. 1, описывающую циклы почти порогового матроида и проверочную матрицу H. При этом C_i соответствует функции f_i ($i = 1,2,...,12$).

Табл. 1.

№ функции	$f_1=x_2$	$f_2=x_1$	$f_3=x_1+x_2$	$f_4=x_1+x_2+1$	$f_5=x_1+x_2+2$	$f_6=x_2-x_1$	$f_7=x_2-x_1+1$	$f_8=x_2-x_1+2$	$f_9=x_1+1$	$f_{10}=x_1+2$	$f_{11}=x_2+1$	$f_{12}=x_2+2$
0	0	0	0	1	2	0	1	2	1	2	1	2
1	0	1	1	2	0	2	0	1	2	0	1	2
2	0	2	2	0	1	1	2	0	0	1	1	2
3	1	0	1	2	0	1	2	0	1	2	2	0
4	1	1	2	0	1	0	1	2	2	0	2	0
5	1	2	0	1	2	2	0	1	0	1	2	0
6	2	0	2	0	1	2	0	1	1	2	0	1
7	2	1	0	1	2	1	2	0	2	0	0	1
8	2	2	1	2	0	0	1	2	0	1	0	1

Итак, циклы матроида, с помощью функции выбора, определяются номерами ненулевых элементов столбцов табл. 1, построенной с помощью линейных функций: C_1={3,4,5,6,7,8}, Z_1={0,1,2}; C_2={1,2,4,5,7,8}, Z_2={0,3,6}; C_3={1,2,3,4,6,8}, Z_3={0,5,7}; C_4={0,1,3,5,7,8}, Z_4={2,4,6}; C_5={0,2,4,5,6,7}, Z_5={1,3,8}; C_6={1,2,3,5,6,7}, Z_6={0,4,8}; C_7={0,2,3,4,7,8}, Z_7={1,5,6}; C_8={0,1,4,5,6,8}, Z_8={2,3,7}; C_9={0,1,3,4,6,7}, Z_9={2,5,8}; C_{10}={0,2,3,5,6,8}, Z_{10}={1,4,7}; C_{11}={0,1,2,3,4,5}, Z_{11}={6,7,8}; C_{12}={0,1,2,6,7,8}, Z_6={3,4,5}. Ранг матрицы H над полем GF(3) равен трем, т.е. таблица СРС имеет $3^9 = 19683$ срок.

Матроиды в схемах разделения секрета на эллиптических кривых

Как было сказано ранее, в работе [6] были описаны СРС при помощи многочленов на эллиптических кривых. В них участники параметризуются точками на эллиптической кривой, а их долями секрета являются значение секретного многочлена в этой точке на кривой. Подход этой статьи – использовать многочлен (третьей степени) на эллиптической кривой для генерации проверочной матрицы над GF(q) кода линейной СРС. Возьмем три конечные точки эллиптической кривой, находящиеся на одной прямой. Сумма этих точек будет равна нулю **0**, т.е. бесконечно удаленной точке кривой [6]. Тогда по теореме о главных дивизорах [5] существует многочлен F третьей степени на эллиптической кривой с корнями в этих точках, т.е. $F(P_i)=0$ (i=1,2,3). При этом эти точки могут совпадать. Таким образом, получается три случая: 1) если $P_1 \neq P_2 \neq P_3 \neq P_1$, то P_1+P_2+P_3=**0**; 2) если P_1=P_2, то 2P_1+P_3=**0** или, если P_2=P_3, то P_1+2P_2=**0**; 3) если P_1=P_2=P_3, то 3P_1=**0**.

Значение многочлена степени три в каждой конечной точке эллиптической кривой определяет строки проверочной матрицы H. При этом ненулевые элементы строк проверочной матрицы H определяют циклы $C = M \setminus Z$ векторного матроида M над GF(q), а нулевые элементы – нуль-множества Z, где M – множество конечных точек кривой над GF(q). Нуль-множества Z задаются прямыми, пересекающимися с эллиптической кривой, при этом сумма точек пересечения прямой, соответствующей нуль-множеству Z, с кривой равна нулю: если $P_1 \neq P_2 \neq P_3 \neq P_1$, то $Z_1 = \{P_1, P_2, P_3\}$, и P_1+P_2+P_3=**0**; если P_1=P_2, то $Z_2 = \{P_1, P_3\}$, и либо 2P_1+P_3=**0**, либо P_1+2P_3=**0**; если P_1=P_2=P_3, то $Z_3 = \{P_1\}$, и 3P_1=**0**.

Проверим выполнение первой аксиомы матроида в терминах антициклов. Поскольку циклы матроида определяются как дополнения нуль-множеств, то потребуем, чтобы в нуль-множествах матроида M не было одноэлементных нуль-множеств. Это означает, что на эллиптической кривой нет точек второго и третьего порядка. Тогда, если нуль-множества определяются по двум или трем различным точкам эллиптической кривой, то эти точки задают единственную прямую. Поэтому антицикла в антицикле, т.е. одной прямой внутри другой прямой, быть не может. Итак, при условии $|Z| \geq 2$, т.е. нуль-множества Z определяются прямыми по двум или трем различным конечным точкам на эллиптической кривой, первая аксиома матроида выполняется.

Проверим выполнение второй аксиомы матроида в терминах циклов. Пусть $Q \in (C_1 \bigcap C_2)$, тогда $F_1(Q) \neq 0$ и $F_2(Q) \neq 0$. Существует ли такой цикл C, что $C \subset (C_1 \bigcup C_2) \setminus Q$? Если прямые, соответствующие нуль-множествам Z_1 и Z_2, не имеют общих точек пересечения на кривой $Z_1 \bigcap Z_2 = \varnothing$, то объединение соответствующих циклов

$C_1 \bigcup C_2$ есть вся кривая без бесконечно удаленной точки кривой, т.е. $C_1 \bigcup C_2 = M$. В этом тривиальном случае вторая аксиома матроида с очевидностью выполняется. Пусть E – конечная точка на эллиптической кривой, тогда через нее и через любую другую точку кривой можно провести прямую, соответствующую нуль-множеству Z_3. Следовательно, во множестве $C_1 \bigcup C_2 = M$ есть цикл $C_3 = M \setminus Z_3$. Если же разные нуль-множества Z_1 и Z_2 пересекаются на кривой, т.е. $Z_1 \bigcap Z_2 \neq \varnothing$, то только в одной точке, иначе они будут совпадать. Поэтому $|Z_1 \bigcap Z_2| = 1$. При этом объединение соответствующих им циклов C_1 и C_2 есть вся кривая кроме бесконечно удаленной точки **0** и точки пересечения P_1 нуль-множеств. Итак, пусть $R = \{P_1\}$, $R = Z_1 \bigcap Z_2$ и $|R| = 1$, тогда $C_1 \bigcup C_2 = M \setminus R$. Пусть точка $Q \notin (Z_1 \bigcup Z_2)$, тогда $P_1 \neq Q$, и во множестве $C_1 \bigcup C_2 \setminus \{Q\} = M \setminus (R \bigcup \{Q\})$ должен содержаться цикл – проверим это. Из $Q \in (C_1 \bigcap C_2)$ вытекает, что прямая P_1Q определяет нуль-множество Z_3, содержащее две различные точки P_1 и Q, так что искомым циклом будет $C_3 = M \setminus Z_3$. Следовательно, вторая аксиома матроида выполняется. Итак, доказано

Утверждение 5. Если на эллиптической кривой нет точек второго и третьего порядка, то множество ее конечных точек M с определенными выше через нуль-множества циклами является матроидом.

Поскольку нуль-множества матроида M определяются прямыми, которые могут иметь две или три различные точки пересечения с эллиптической кривой, то отсюда вытекает

Утверждение 6. Мощность циклов матроида M равна либо $N-4$, если $|Z| = 3$, либо $N-3$, если $|Z| = 2$, где N=|GEC(GF(q))|.

Из утверждения 6 следует, что при помощи многочлена на эллиптической кривой реализуется линейная идеальная совершенная почти пороговая СРС.

Пример реализации идеальной совершенной почти пороговой СРС при помощи эллиптических кривых над GF(3)

Рассмотрим эллиптическую кривую $y^2 = x^3 - 4x + 4$ над полем GF(3). Всего эта кривая имеет $G = EC(GF(3)) = 7$ точек, включая бесконечно удаленную, которые образуют абелеву группу. При этом группа G изоморфна Z_7, т.е. $G \cong Z_7$, поэтому каждую точку кривой можно сопоставить с вычетом по модулю семь. Конечным точкам соответствуют ненулевые вычеты, так что $M = \{1,2,3,4,5,6\}$. В силу этого изоморфизма будем обозначать точки так: **1**=(2;2), **2**=(0;2), **3**=(1;1), **4**=(1;2), **5**=(0;1), **6**=(2;1)=**-1**. Тогда возможны три варианта: 1) P_1+P_2=**0**, deg$F$=2; 2) 2P_1+P_2=**0**, deg$F$=3; 3) P_1+P_2+P_3=**0**, deg$F$=3. Определим, какие нуль-множества будут соответствовать этим трём вариантам, при этом **0** не учитывается:

1) P_1+P_2=**0**, Z_1={**1**,**6**}; Z_2={**2**,**5**}; Z_3={**3**,**4**};

2) 2P_1+P_2=**0**, Z_4={**1**,**5**}; Z_2={**2**,**3**}; Z_6={**3**,**1**}; Z_7={**4**,**6**}; Z_8={**5**,**4**}; Z_9={**6**,**2**};

3) P_1+P_2+P_3=**0**, Z_{10}={**1**,**2**,**4**}; Z_{11}={**3**,**5**,**6**}={**-1**,**-2**,**-4**}.

Циклами матроида *M* будут дополнения этих нуль-множеств $C = M \setminus Z$:

1) C_1={**2**,**3**,**4**,**5**}; C_2={**1**,**3**,**4**,**6**}; C_3={**1**,**2**,**5**,**6**};

2) C_4={**2**,**3**,**4**,**6**}; C_2={**1**,**4**,**5**,**6**}; C_6={**2**,**4**,**5**,**6**}; C_7={**1**,**2**,**3**,**5**}; C_8={**1**,**2**,**3**,**6**}; C_9={**1**,**3**,**4**,**5**};

3) C_{10}={**3**,**5**,**6**}; C_{11}={**1**,**2**,**4**}.

Нетрудно проверить непосредственно, что обе аксиомы матроида выполняются. Приведем первый шаг реализации такой СРС – определим проверочную матрицу кода *H*:

$$H^T = \begin{pmatrix} 0 & 2 & 1 & 0 & 1 & 0 & 2 & 1 & 2 & 0 & 1 \\ 1 & 0 & 2 & 2 & 0 & 1 & 1 & 2 & 0 & 0 & 1 \\ 2 & 1 & 0 & 2 & 0 & 0 & 1 & 1 & 2 & 2 & 0 \\ 2 & 1 & 0 & 1 & 2 & 2 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 2 & 0 & 1 & 2 & 2 & 0 & 1 & 2 & 0 \\ 0 & 2 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 2 & 0 \end{pmatrix}$$

Ранг матрицы *H* над GF(3) равен трем, т.е. таблица СРС имеет $3^3 = 27$ срок.

Рассмотрим, как строились строки матрицы *H*. Для первого случая (P_1+P_2=**0**), т.е. первые три строки матрицы *H*, прямая, определяющая нуль-множество, вертикальна, что даёт многочлен вида $F(P) = x - x_0$. Так, в первой строке x_0 равна абсциссе первой (или шестой) точки эллиптической кривой, так как Z_1={**1**,**6**}, **-1=6**, т.е. $x_0 = 2$. Далее, для каждого элемента первой строки рассчитывается значение $F(P) = x_i - 2$, где x_i $(1 \le i \le 6)$ – значение абсциссы точки соответствующей номеру столбца с 1 до 6.

Для второго (2P_1+P_2=**0**) и третьего (P_1+P_2+P_3=**0**) случая, т.е. с четвертой по девятую строку и последние две строки соответственно, рассчитывалось значение функции $F(P) = (kx + b) - y$. Так, для расчета четвертой строки матрицы *H* параметры *k* и *b* находятся из системы двух линейных уравнений и Z_4={**1**,**5**}: $\begin{cases} 2 = k \cdot 2 + b \\ 1 = k \cdot 0 + b \end{cases}$. Отсюда *k*=2 и *b*=1. Далее, для каждого элемента четвертой строки рассчитывается значение $F(P) = (2x_i + 1) - y_i$, где x_i, y_i $(1 \le i \le 6)$ – значение абсциссы и ординаты точки, соответствующей номеру столбца с 1 до 6. Аналогичные расчеты производились и в третьем случае.

Заключение

В данной работе рассмотрен двойственный вариант аксиоматизации матроидов с помощью антициклов – нуль-множеств. Доказано, что реализуется бесконечная серия

матроидов M на m-мерном проективном и аффинном пространстве над GF(q) с одинаковой мощностью циклов $|C| = |M \setminus Z|$. Показана реализация идеальной совершенной почти пороговой СРС на эллиптической кривой, на которой многочлен третьей степени используется для генерации проверочной матрицы над GF(q) кода линейной СРС.

Список литературы

1. Асанов М.О., Баранский В.А., Расин В.В. Дискретная математика: графы, матроиды, алгоритмы. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. – 288 с.
2. Блейкли Г.Р., Кабатянский Г.А. Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Проблемы передачи информации. – 1997. – Т. 33, № 3. – С. 102-110.
3. Доктрина информационной безопасности [Электронный ресурс]. – Российская газета: http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm (дата обращения 27.04.2012)
4. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: Изд. Урал. Ун-та, 2003. – 328 с.
5. Кнэпп Э. Эллиптические кривые. – М.: Факториал Пресс, 2004. – 488 с.
6. Медведев Н.В., Титов С.С. Почти пороговые схемы разделения секрета на эллиптических кривых // Доклады Томского государственного университета систем управления и радиоэлектроники. – Томск: Издательство Томского государственного университета систем управления и радиоэлектроники. – 2011. – № 1 (23), ч. 1. – С. 91-96.
7. Холл М. Комбинаторика. – М.: Издательство «МИР», 1970. – 424 с.
8. Введение в криптографию / Под общ. ред. В.В. Ященко. – СПб: Питер, 2001. – 288 с.

Рецензенты:

Баутин Сергей Петрович, доктор физ.-мат. наук, профессор, профессор кафедры «Высшая и прикладная математика». Уральский государственный университет путей сообщения, г.Екатеринбург.

Ялышев Юрий Иванович, доктор физ.-мат. наук, профессор, и.о. заведующего кафедрой «Информационные технологии и защита информации», проректор по информатизации. Уральский государственный университет путей сообщения, г.Екатеринбург.