Kosenko Evgeny Yurevich – e-mail: ekosenko@sfedu.ru; cand. of eng. sc.; associate professor; senior researcher.

Medvedev Mikhail Yurjevich – e-mail: medvmihal@sfedu.ru; dr. of eng. sc.; leading researcher.

Pshikhopov Viacheslav Khasanovich – e-mail: pshichop@rambler.ru; dr. of eng. sc.; professor; director.

Mamchenko Mark Vladislavovich – V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences; e-mail: markmamcha@gmail.com; Moscow, Russia; phone: +74953348910; researcher.

УДК 004 DOI 10.18522/2311-3103-2021-1-218-235

Ю.Н. Кочеров, Д.В. Самойленко

РАЗРАБОТКА НАДЕЖНОГО МЕТОДА СВЯЗИ РТК НА БАЗЕ ГРУППОВОГО МЕТОДА РАЗДЕЛЕНИЯ ДАННЫХ, ОСНОВАННОГО НА СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

В работе рассматривается надежный метод передачи данных в системах связи и управления роботехническими комплексами. В связи с тем, что изменение части закодированной информации передаваемой по каналам связи может привести к частичной или полной потере данных и, как следствие, привести к потере контроля над роботехническим комплексом. Следовательно, необходимо применять методы защиты данных, передаваемых по радиоканалам. Предлагаемый метод предназначается для обеспечения защиты информации в каналах связи роботехнических комплексов от доступа несанкционированных пользователей и подтверждения достоверности полученной информации. В статье исследуются методы защиты данных, предназначенных для защиты информации, циркулирующей в системах образованных несколькими взаимодействующими агентами. Рассматриваемый подход базируется на методах защиты информации и помехоустойчивого кодирования основанных на системе остаточных классов. Применяемые методы помехоустойчивого кодирования, основанные на системе остаточных классов, базируются на идее порогового разделения данных, в которых исходную информацию можно восстановить имея k из n частей исходной информации. Это связано с тем, что избыточная модулярная арифметика, или избыточная система остаточных классов, обладает уникальными свойствами относительно обнаружения и коррекции ошибок. Кроме того, система остаточных классов обладает таким преимуществом как низкая вычислительной сложность алгоритмов разделения данных. Для увеличения надежности связи роботехнических комплексов в мультиканальных системах связи в работе предложен метод защиты информации и помехоустойчивого кодирования, основанный на многоступенчатом пороговом разделении данных. В результате работы получена система помехоустойчивой передачи информации, обеспечивающая комплексную защиту роботехнических комплексов.

Система остаточных классов; надежность передачи данных; пороговое разделение данных; обеспечение надежной связи роботехнических комплексов.

Y.N. Kocherov, D.V. Samoylenko

DEVELOPMENT OF A RELIABLE RTC COMMUNICATION METHOD BASED ON A GROUP DATA SEPARATION METHOD BASED ON A RESIDUAL CLASS SYSTEM

The paper considers a reliable method of data transmission in commu-nication systems and control of robotic complexes. Due to the fact that a change in part of the encoded information transmitted through com-munication channels can lead to partial or complete loss of data and, as a consequence, lead to loss of control over the robotic complex. There-fore, it is necessary to ap-

ply methods of protecting data transmitted over radio channels. The proposed method is intended to ensure the protection of information in the communication channels of robotic complexes from the access of unauthorized users and to confirm the reliability of the information received. The article examines data protection methods designed to protect in-formation circulating in systems formed by several interacting agents. The approach under consideration is based on the methods of infor-mation protection and error-correcting coding based on the system of residual classes. The applied methods of error-correcting coding, based on the system of residual classes, are based on the idea of threshold data separation, in which the original information can be restored from parts of the original information. This is due to the fact that redundant modular arithmetic, or redundant system of residual classes, has unique properties with re-spect to error detection and correction. In addition, the system of resid-ual classes has such an advantage as low computational complexity of data separation algorithms. To increase the reliability of communication between robotic complex-es in multichannel communication systems, the paper proposes a meth-od for information protection and noise-resistant coding, based on a multistage threshold data separation. As a result of the work, a system of noise-resistant information trans-mission was obtained, which provides comprehensive protection for robotic systems.

System of residual classes; reliability of data transmission; threshold data separation; ensuring reliable communication of robotic complexes.

1. Введение. Мобильные роботехнические комплексы (МРК) решают такие задачи как: разведка и наблюдение; уничтожение важных объектов; нейтрализация взрывоопасных объектов, минных заграждений; поисковые и аварийно-спасательные работы и др. Так как рассмотренные выше задачи сложно подаются формализации то во главу угла стает задача дистанционного управления роботехническими комплексами (РТК). Каналы связи РТК на основе радиопередач подвергаются различным электромагнитным воздействиям как техногенного характера, так и третьей стороны (несанкционированных пользователей), которая может воздействовать на РТК и как результат оператор может потерять управление им.

В связи с вышесказанным возникают задачи надежного мультиканального управления роботехническими комплексами.

Для решения такой задачи применяются методы многоканальной маршрутизации. Такая маршрутизация должна обеспечивать высокую пропускную способность и малое время задержки. В основу построения многоканальных систем связи положен принцип уплотнения линий связи. Самым распространенным методом уплотнения является частотное уплотнение при коттором по каждому каналу отводится определенная часть области частот, занимаемая трактом групповой передачи сообщения. При этом необходимо обеспечивать безопасность и надежность информации по каждому каналу.

Для разделения информации по каналам связи принято применять пороговые схемы разделения данных. При этом по каждому каналу передается только часть информации [1].

Такие схемы применяются в том случае, когда существует большая вероятность компрометации одного или нескольких участников, но вероятность предварительного сговора участников считается пренебрежимо малой.

Концепция порогового разделения секрета предложена 1979 израильским криптоаналитиком Ади Шамиром.

В современных алгоритмах для разделения информации на части применяют методы, основанные на системе остаточных классах (СОК). СОК – это непозиционная система счисления, основанная на модулярной арифметике [2, 3]. Представление чисел в СОК основано на понятии вычета и Китайской теореме об остатках [4].

Методы, основанные на СОК, обладают следующими преимуществами:

- СОК обладает корректирующими свойствами [5];
- низкая вычислительная сложность.

Для разработки интеллектуальных РТК необходимо решить следующие вопросы:

1. Низкая робастность существующих адаптивных систем управления роботов для их применения в динамических средах:

♦ модернизация методов адаптивного управления движением роботов и их коллективов (мультиагентные робототехнические системы) в условиях неопределенности и существенных внешних возмущений;

♦ разработка баз данных реального времени для представления знаний в робототехнических комплексах;

♦ создание методов интеллектуального анализа, управления и прогнозирования функционирования робототехнических систем;

♦ разработка методов, схем и процедур обнаружения неисправностей и отказов систем управления робототехническими системами, а также статистического анализа этих отказов.

2. Развитие интерфейсов «человек-робот» в задаче коллаборации при совместном выполнении сложных задач:

♦ развитие новых неинвазивных сенсорных систем, включая силомоментное очувствление, электромиографию и электроэнцефалографию;

♦ разработка алгоритмов распознавания и синтеза естественной речи;

♦ синтез алгоритмов распознавания специфических сценариев поведения человека по визуальной информации с целью мониторинга состояния рабочих, хронических больных и престарелых людей, а также предотвращения агрессии в общественных местах;

♦ развитие методов скоростного обучения роботов (тренажеров).

3. Организация обратной связи, предоставляющей полную и значимую информацию о состоянии окружения и самой робототехнической системы:

♦ разработка высокоэффективных, малогабаритных и дешевых систем технического зрения для робототехнических систем;

♦ разработка малогабаритных высокоточных датчиков силомоментной информации для робототехнических систем;

♦ развитие методов обработки сенсорной информации для задач одновременной локализации и картирования;

4. Отсутствие эффективных способов передвижения и способов воздействия на внешние объекты. Развитие бионических технологий в робототехнике:

♦ разработка новых принципов перемещения в пространстве (использование ветра, волн, течений, планирование в воде или восходящих потоках воздуха и т.п.);

♦ разработка новых принципов воздействия на объекты (использование для манипуляций и воздействий электромагнитного поля, потоков газа или жидкости, электрических разрядов и т.п.).

♦ создание и развитие новых типов движителей и систем анализа данных, основанных на бионических принципах (рыбьи плавники, глаза стрекозы, крылья бабочки и т.п.).

5. Координированное управление коллективами роботов (мультиагентные РТК), обеспечение надежной и бесперебойной связи в робототехнических системах, самообучение и самопрограммирование:

♦ прецизионное манипулирование крупногабаритными и массивными объектами;

♦ разработка алгоритмов распределения задач между агентами системы с учетом их текущего состояния;

♦ фундаментальные проблемы связи при когерентной работе группы роботов, в том числе с децентрализованным управлением.

2. Обзор методов порогового разделения данных. В криптографии под термином разделение секрета понимается любой из способов распределения секрета среди группы участников каждому из которых достается только своя доля.

Простейшим методом реализации подобной схемы является следующий пример:

♦ пусть существует группа из n участников схемы разделения секрета и сообщение S длинной l состоящее из набора двоичных символов. Подобрав случайным образом набор двоичных сообщений S_1, S_2, S_3, S_4,…,S_n таких, что в сумме будут давать S и распространив среди всех участников схемы разделения секрета, то восстановить секрет будет возможно только в том случае, когда n участников соберутся вместе.

Пороговое разделение секрета отличается от процедуры разбиения тем, что для восстановления исходной информации потребуется только k из n исходных частей, на которые секрет был разделен.

Идею таких схемы независимо друг от друга предложили в 1979 г. Адди Шамир и Джордж Блэкли.

В таких схемах под понятием разрешенная коалицией понимают такое количество участников, которые имеют достаточное количество долей для восстановления секрета

Пороговая схема Шамира построена вокруг концепции полиномиальной интерполяции. Главная идея этой концепции состоит в том, что интерполяция невозможна если известно меньшее количество точек. Другими словами, через две точки на плоскости можно построить неограниченное количество кривых степени 2, и чтобы построить через из них единственно верную кривую нужна третья точка (рис. 1).

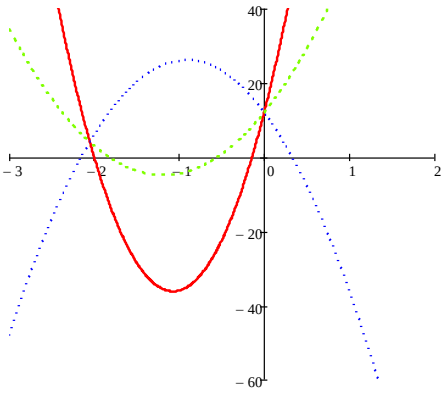

Рис. 1. Графическая иллюстрация схемы Шамира

Для разделения секрета межу n пользователями таким образом, чтобы восстановить информацию с помощью k частей, секрет подставляют в качестве свободного члена полинома $k-1$ степени.

Восстановить этот полином, а следовательно, и сам секрет можно только по k точкам.

Для оценки временных затрат рассмотрим вычислительную сложность алгоритма разделения данных на основе схемы Шамира. Асимптотическая поразрядная оценка сложности этого алгоритма выражается как:

$$O_B(\log_2^3(n)+\log_2^2(n^2)+\sum_{i=0}^{\lfloor \log_2(N+1)\rfloor+1}\log_2(2\cdot n^2+i)), \quad (1)$$

где n – максимальное значение числа в десятичном представлении; N – порядок полинома.

На рис. 2 приведен принцип вычисления с применением двоичного каскадного сумматора и вычислительной сложностью на каждом уровне для полинома второй степени.

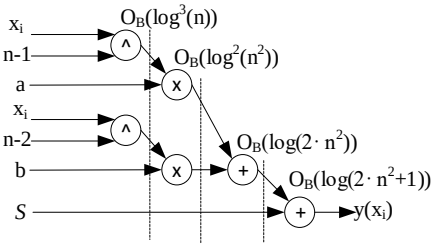

Рис. 2. Вычисление части информации схемой Шамира

Джордж Блэкли предложил свою схему, основанную на принципе векторного разделения секрета.

В такой схеме секретом является одна из координат k-мерной плоскости в k-мерном пространстве. Частями разделяемого секрета является уравнения $k-1$ мерных гиперплоскостей.

Основная концепция схемы разделения секрета Блэкли заключается в следующем: пересечением $k-1$ линейно независимых уравнений плоскостей $k-1$ порядка является прямая; пересечением k линейно независимых плоскостей $k-1$ порядка является точка. Одна из координат пересечения $k-1$ мерных плоскостей в k-мерном пространстве и будет разделяемым секретом.

Схема Блэкли для $k=3$ представлена на рис. 3.

Для оценки временных затрат рассмотрим вычислительную сложность алгоритма разделения данных на основе схемы Блэкли. Асимптотическая поразрядная оценка сложности этого алгоритма выражается как:

$$O_B(\log_2^2(n)+\sum_{i=0}^{\lfloor \log_2(N+1)\rfloor+1}\log_2(2\cdot n^2+i)), \quad (2)$$

где n – максимальное значение числа в десятичном представлении; N – порядок уравнения плоскости.

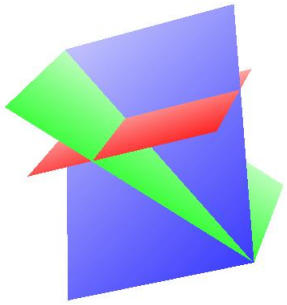

Рис. 3. Схема разделения секрета Блэкли

На рис. 4 приведен принцип вычисления с применением двоичного каскадного сумматора и вычислительной сложностью на каждом уровне для уравнения плоскости третьей степени.

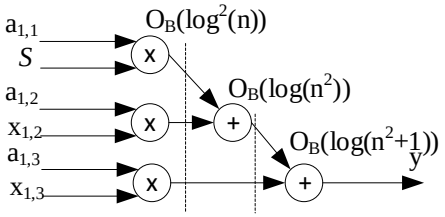

Рис. 4. Вычисление части информации схемой Блэкли

На рис. 5 показаны графики асимптотической поразрядной оценка сложности схем Блэкли и Шамира от порядка уравнений.

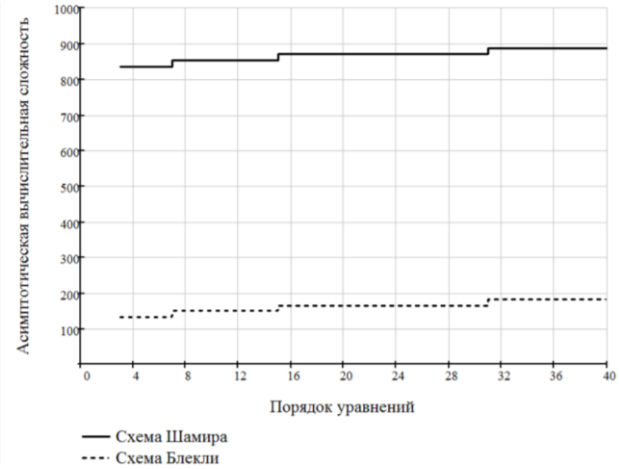

Рис. 5. Оценка вычислительной сложности схем Блэкли и Шамира

О отличие от схемы Шамира и Блэкли принцип которых основывается на расчетах уравнений полинома или плоскости существуют другие методы разделения данных, которые основаны на вычисления остатков целочисленного деления информации на ряд оснований.

СОК определяется рядом попарно взаимно простых модулей $(p_1, p_2, p_3, ..., p_n)$, таких, что $gnd(p_i, p_j) = 1(\forall : i, j = 0,1,2,...,n; i \neq j)$ называемых базисом при $P = p_1 \cdot p_2 \cdot ... \cdot p_n$ таким образом любому целому S из множества $[0; P-1]$ ставится соответствие набор остатков $(\alpha_1, \alpha_2, ..., \alpha_n)$ где:

$$\begin{cases} \alpha_1 = S \bmod p_1 \\ \alpha_2 = S \bmod p_2 \\ \quad ... \\ \alpha_n = S \bmod p_n \end{cases}.$$

При этом Китайская теорема об остатках гарантирует однозначность представления целых положительных чисел из диапазона $[0; P-1]$.

Принципы Китайкой теоремы об остатках были также применены для разделения секрета и предложены в работах: M. Mignotte. How to Share a Secret // Lecture Notes in Computer Science. – 1983. – Vol. 149. – P. 371-375. – Doi:10.1007/3-540-39466-4_27. и C.A. Asmuth and J. Bloom. A modular approach to key safeguarding // IEEE Transactions on Information Theory. – 1986. – Vol. 2. – P. 208-210.

Схема разделения Миньотта [6] позволяет пользователю, имеющему некоторое разрешенное количество частей информации, восстановить ее, причем единственным образом.

Принцип работы схемы, следующий: пусть необходимо разделить информацию S среди n пользователей таким образом чтобы при условии наличия k частей, было возможно восстановить исходную информацию, а имея в наличие $k-1$ не имели такой возможности.

Для этого необходима последовательность натуральных чисел (называемую (k,n) –последовательностью Миньотта) такая, что: $p_1 < p_2 < ... < p_n$ и $\prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i$. Причем должны соблюдаться следующие условия:

- любые два числа последовательности должны быть взаимно простыми т.е. $gnd(p_i, p_j) = (\forall : i, j = 0,1,2,...,n; i \neq j)$;
- информация должна находится в диапазоне $\alpha < S < \beta$ где $\alpha = \prod_{i=1}^{k} p_i$, а $\beta = \prod_{i=1}^{k-2} p_{n-i}$ то есть $p_1 \cdot p_2 \cdot ... \cdot p_k < S < p_{n-k+2} \cdot p_{n-k+3} \cdot ... \cdot p_n$.

Части вычисляются по формуле $\alpha_i = S \bmod p_i$ для всех $i \in [1;n]$ и распределяются по каналам связи.

Для оценки временных затрат рассмотрим вычислительную сложность алгоритма разделения данных на основе схемы Блэкли. Асимптотическая поразрядная оценка сложности этого алгоритма выражается как:

$$O_B(\log_2^2(n)), \quad (3)$$

Схема Асмута-Блума [7], как и схема Миньотта это пороговая схема разделения секрета, построенная с использованием ряда простых чисел которая позволяет разделить секрет серели n сторон так что его восстановят любые k участников.

Для разделения секрета схемой Асмута-Блума необходимо выбрать простое число q больше $[8, 9]$ S .

Следующим этапом проводится выбор n взаимно простых друг с другом чисел $p_1, p_2, ..., p_n$ удовлетворяющих следующим условиям:

- $\forall i : q < p_i$;
- $\forall i : p_i < p_{i+1}$;
- $p_1 \cdot p_2 \cdot ... \cdot p_k < q \cdot p_{n-k+2} \cdot p_{n-k+3} \cdot ... \cdot p_n$ [10].

Далее необходимо выбрать случайное число r и вычислить $S' = S + r \cdot q$.

Части секрета вычисляются по формуле $\alpha_i = S' \bmod p_i$. Участникам раздается следующая информация $\{q, p_i, \alpha_i\}$.

Для оценки временных затрат рассмотрим вычислительную сложность алгоритма разделения данных на основе схемы Асмута-Блума. Асимптотическая поразрядная оценка сложности этого алгоритма выражается как:

$$O_B(\log_2^2(n)+\log_2(n^2)), \quad (4)$$

Как видно из формул (3) и (4) вычислительная сложность алгоритмов, основанных на СОК, зависит только от максимального значения числа. Из формул (1) и (2) видно, что вычислительная сложность зависит от размера числа и порядка полинома или порядка уравнения плоскости. На рис. 6 показана зависимость асимптотической вычислительной сложности рассмотренных алгоритмов от размера числа при разделении на 3 части. При увеличении количества частей в схемах основанных на системе остаточных классов вычислительная сложность изменяться не будет, а в схемах Блэкли и Шамира будет увеличиваться в соответствии с рис. 5.

Из графика рис. 6 можно сделать вывод что для разделения данных по показателю вычислительная сложность следует применять пороговые алгоритмы, основанные на СОК.

Для схем разделения данных существуют также такие показатели как совершенность и идеальность:

- ♦ схемы разделения секрета, в которых разрешенные коалиции участников могут однозначно восстановить секрет, а неразрешенные не получают никакой апостериорной информации о возможном значении секрета, называются совершенными;
- ♦ схема разделения секрета называется идеальной, если размер доли секрета равен размеру самого секрета.

Так как в схеме Миньотта части вычисляются $\alpha_i = S \bmod p_i$ то можно сделать вывод что эта схем не совершенная и не идеальная. Поэтому в этой работе будет применяться схема Асмута-Блума.

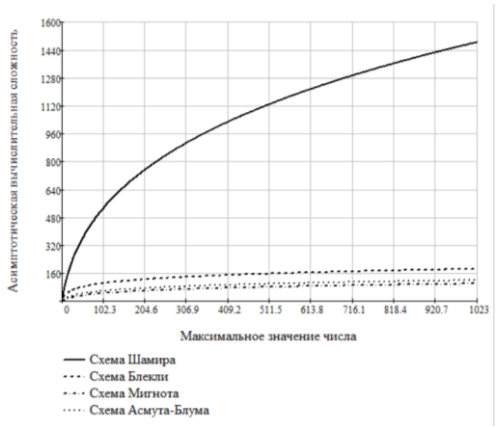

Рис. 6. Оценка вычислительной сложности схем рассмотренных алгоритмов

3. Оценка методов восстановления данных из системы остаточных классов в позиционную систему счисления. При восстановлении чисел из СОК в позиционную систему счисления (ПСС) могут применяться различные методы такие как: методы основанные на КТО; метод Гарнера [11] (метод, основанный на обобщенной полиадической системе счисления (ОПСС)) или метод совместного использования КТО и ОПСС [12, 13].

Восстановление исходной информации с применением КТО основывается на вычислении значения по формуле:

$$S = \left| \sum_{i=1}^{n} \alpha_i B_i \right|_P$$

где $\alpha_i = S \bmod p_i$; B_i – ортогональные базисы, рассчитываемые по формуле $B_i = \frac{m_i P}{p_i}$, m_i – положительные, целые числа называемые весами базиса, их, определяют из приближения $P_i m_i = 1 \bmod p_i$.

Рассмотрим пример (k, n) при $k = 3$ и $n = 5$ порогового разделения данных и их восстановления с применением метода основанного на КТО.

Пусть дано число $S = 200$ из условий: $\forall i : q < p_i$; $\forall i : p_i < p_{i+1}$; $p_1 \cdot p_2 \cdot \ldots \cdot p_k < q \cdot p_{n-k+2} \cdot p_{n-k+3} \cdot \ldots \cdot p_n$ примем следующие значения $q = 257$, $p_1 = 271$, $p_2 = 277$, $p_3 = 281$, $p_4 = 283$, $p_5 = 293$. Выбирается случайное число $r = 25$. Тогда:

$$S^{'} = S + r \cdot q = 200 + 25 \cdot 257 = 6625.$$

Следующим этапом $S^{'} = 6625$ разделяется на $n = 5$ частей:

$$\alpha_1 = S^{'} \bmod p_1 = 6625 \bmod 271 = 121;$$

$$\alpha_2 = S^{'} \bmod p_2 = 6625 \bmod 277 = 254;$$

$$\alpha_3 = S^{'} \bmod p_3 = 6625 \bmod 281 = 162;$$

$$\alpha_4 = S^{'} \bmod p_4 = 6625 \bmod 283 = 116;$$

$$\alpha_5 = S^{'} \bmod p_5 = 6625 \bmod 293 = 171.$$

Части α_1, α_2, α_3, α_4, α_5 передаются по разным каналам передачи информации [14, 15].

Далее рассмотрен пример восстановления информации по $k = 3$ частям. Для восстановления будут использоваться следующие части: $\alpha_1 = 121$; $\alpha_3 = 162$; $\alpha_5 = 171$.

Тогда диапазон СОК $P = p_1 \cdot p_3 \cdot p_5 = 271 \cdot 281 \cdot 293 = 22312243$. Следующим этапом вычисляются коэффициенты:

$$P_1 = \frac{P}{p_1} = \frac{22312243}{271} = 82333;$$

$$P_3 = \frac{P}{p_1} = \frac{22312243}{281} = 79403;$$

$$P_5 = \frac{P}{p_5} = \frac{22312243}{293} = 761511.$$

Из приближения $P_i m_i \bmod p_i \equiv 1$ рассчитываются веса базиса:

$$82333 m_1 \bmod 271 \equiv 1 \; тогда \; m_1 = 85;$$

$$79403 m_3 \bmod 281 \equiv 1 \; тогда \; m_3 = 96;$$

$$761511 m_5 \bmod 293 \equiv 1 \; тогда \; m_1 = 101.$$

Тогда веса базисов равны:

$$B_1 = P_1 \cdot m_1 = 82333 \cdot 85 = 6998305;$$

$$B_3 = P_3 \cdot m_3 = 79403 \cdot 96 = 7622688;$$

$$B_5 = P_5 \cdot m_5 = 76151 \cdot 101 = 7691251.$$

Тогда:

$$S^{'} = (B_1 \cdot \alpha_1 + B_3 \cdot \alpha_3 + B_5 \cdot \alpha_5) \bmod P =$$

$$= (121 \cdot 6998305 + 162 \cdot 7622688 + 171 \cdot + 7691251) \bmod 22312243 = 6625,$$

а $S = S^{'} - r \cdot q = 6625 - 25 \cdot 257 = 200$ [16].

Недостаток этого метода, заключается в том, что для преобразования из системы СОК в позиционную систему счисления требуется операции умножение и сложение больших чисел и нахождение остатка по модулю P.

Для снижения вычислительной сложности стоит применять метод Гарнера в котором операция нахождение остатка вычисляется не от полного диапазона, а по множеству p_i.

В методе Гарнера используется полиадическая система счисления, где любое число представляется в системе взаимно простых чисел $p_1, p_2, ..., p_n$ следующим образом:

$$S = a_1 + a_2 \cdot p_1 + a_3 \cdot p_1 \cdot p_2 + \ldots + a_n \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n \text{ [15].}$$

Коэффициенты a_i, $i = [0; n]$ вычисляются следующим образом:

$$a_i = \alpha_i \bmod p_i;$$

$$a_2 = (\alpha_2 - a_1)\tau_{12} m \bmod p_2;$$

$$a_3 = ((\alpha_3 - a_1)\tau_{13} - a_2)\tau_{23} \bmod p_3;$$

$$\ldots$$

$$a_n = ((...(\alpha_n - a_1)\tau_{1n} - a_2)\tau_{2n} - ... - a_{1n})\tau_{n-1n} \bmod p_n.$$

Константы τ_{kj} рассчитываются из условий:

$$\tau_{kj} = \left| \frac{1}{p_k} \right|_{p_j} \text{ где } 1 \le k < j \le n.$$

Подставив константы τ_{kj}, получим:

$$a_i = \alpha_i \bmod p_i;$$

$$a_2 = ((p_1^{-1}) \bmod p_2 (\alpha_2 - a_1)) \bmod p_2;$$

$$a_3 = ((p_2^{-1}) \bmod p_3 ((p_1^{-1}) \bmod p_3 (\alpha_3 - a_1) - a_2)) \bmod p_3;$$

$$\ldots$$

Далее рассмотрен пример восстановления информации по $k = 3$ частям. Для восстановления будут использоваться те же, как и в предыдущем примере: $\alpha_1 = 121$; $\alpha_3 = 162$; $\alpha_5 = 171$.

Для того рассчитаны константы $\tau_{kj} = \left| \frac{1}{p_k} \right|_{p_j}$ где $1 \le k < j \le n$:

$$\tau_{12} = \left|\frac{1}{p_1}\right|_{p_2} = \left|\frac{1}{271}\right|_{281} = 28;$$

$$\tau_{13} = \left|\frac{1}{p_1}\right|_{p_3} == \left|\frac{1}{271}\right|_{293} = 253;$$

$$\tau_{23} = \left|\frac{1}{p_2}\right|_{p_3} == \left|\frac{1}{281}\right|_{293} = 122.$$

Рассчитываем коэффициенты ОПСС:

$$a_1 = \alpha_1 \bmod p_1 = 121 \bmod 271 = 121;$$

$$a_2 = (\alpha_2 - a_1)\cdot \tau 12 \bmod p_2 = (162 - 121)\cdot 28 \bmod 281 = 24;$$

$$a_3 = ((\alpha_3 - a_1)\cdot \tau_{13} - a_2)\cdot \tau_{23} \bmod p_2 =$$

$$((179 - 24)\cdot 253 - 24)\cdot 122 \bmod 293 = 0.$$

Тогда:

$$A = a_1 + a_2 \cdot p_1 + a_3 \cdot p_1 \cdot p_2 = 121 + 24 \cdot 271 + 0 \cdot 271 \cdot 281 = 6625.$$

Недостатком метода Гарнера является то, что в каждой итерации применяются операции вычитания и умножения по модулю p_i.

Метод, основанный на совместном применении, КТО и ОПСС исключает операцию вычитания.

Для решения этим методом ортогональные базисы необходимо представить в ОПСС:

$$b_i = b_{i1} + b_{i2} \cdot p_1 + b_{i3} \cdot p_1 \cdot p_2 + ... + b_{in} \cdot p_1 \cdot p_2 \cdot ... \cdot p_n.$$

где b_{ij} – это коэффициенты ОПСС; $i, j = 1, 2, ..., n$.

В связи с тем, что $b_i \bmod p_i = 0$, $\forall : j > i$, то перед первым значащим значением будет $i - 1$ нулей.

Для удобства базисы можно представить в виде матрицы размерностью $[n, n]$.

$$\begin{bmatrix} b_{11} & b_{12} & ... & b_{1n} \\ 0 & b_{22} & ... & b_{2n} \\ ... & ... & ... & ... \\ 0 & 0 & ... & b_{nn} \end{bmatrix}.$$

Тогда

$$S = \begin{bmatrix} |\alpha_1 \cdot b_{11}|^+_{p1} & |\alpha_1 \cdot b_{12}|^+_{p2} & ... & |\alpha_1 \cdot b_{1n}|^+_{pn} \\ 0 & |\alpha_2 \cdot b_{22}|^+_{p2} & ... & |\alpha_2 \cdot b_{21}|^+_{pn} \\ ... & ... & ... & ... \\ 0 & 0 & ... & |\alpha_n \cdot b_{nn}|^+_{pn} \end{bmatrix}.$$

При этом $\alpha_i = \left|\sum_{\substack{i=1 \\ j=1}}^{n} \alpha_i b_{ij}\right|_{p_i}$.

Далее рассмотрен пример восстановления информации по $k=3$ частям [17, 18]. Для восстановления будут использоваться те же, как и в предыдущем примере: $\alpha_1=121$; $\alpha_3=162$; $\alpha_5=171$ [19].

Представим базисы B_i в ОПСС, тогда b_{ij}:

$$b_{11}=1; b_{12}=253; b_{13}=91;$$
$$b_{21}=0; b_{22}=28; b_{23}=100;$$
$$b_{31}=0; b_{32}=0; b_{33}=101;$$

Отсюда:

$$S^{'}=\begin{bmatrix}121\\162\\171\end{bmatrix}\cdot\begin{bmatrix}|1|^{+}_{271} & |253|^{+}_{281} & |91|^{+}_{293}\\ |0|^{+}_{271} & |28|^{+}_{281} & |100|^{+}_{293}\\ |0|^{+}_{271} & |0|^{+}_{281} & |101|^{+}_{293}\end{bmatrix}=\begin{bmatrix}121 & 265 & 278\\ 0 & 40 & 101\\ 0 & 0 & 206\end{bmatrix}$$

$a_1=121, a_2=24, a_3=0.$

$A=a_1+a_2\cdot p_1+a_3\cdot p_1\cdot p_2=121+24\cdot 271+0\cdot 271\cdot 281=6625$

Из вышесказанного можно сделать вывод о привлекательности для практической реализации метода совместного использования КТО и ОПСС.

4. Метод разделения данных на множество подгрупп. Для повышения надежности схем разделения данных внедряется алгоритм разделения на множество подгрупп (рис. 7).

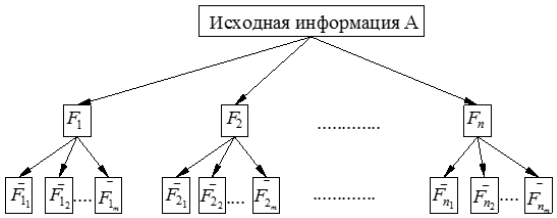

Рис. 7. Структурная схема разделения данных на множество подгрупп

Ниже представлена работа алгоритма с разделением на множество подгрупп. Она состоит из двух этапов [20]:

1) Информация S разделяется на множество, состоящее из n частей «лидеров групп» $F_1, F_2, ..., F_n$.

2) Каждый «лидер группы» $F_1, F_2, ..., F_n$ разделяется на свое новое множество, состоящее из m частей $(F_{1_1}, F_{1_2}, ..., F_{1_m})(F_{2_1}, F_{2_2}, ..., F_{2_m})...(F_{n_1}, F_{n_2}, ..., F_{n_m})$.

Полученные $n\times m$ частей информации $(F_{1_1}, F_{1_2}, ..., F_{1_m})(F_{2_1}, F_{2_2}, ..., F_{2_m})...(F_{n_1}, F_{n_2}, ..., F_{n_m})$ передаются по линиям связи на удаленные сервера.

При хранении и передаче информации возможно использовать СОК. Для этого исходная информация будет разделена на части согласно количеству оснований СОК.

Для надежного хранения и передачи рассчитанных данных вводятся избыточные основания, тем самым увеличивается избыточность информации. В результате этого получаем классическую пороговую схему разделения данных, где для восстановления информации достаточно получить от k групп K частей. Из-

быточность введенной информации позволяет локализовать скомпрометировавшие себя хранилища информации и заблокировать их для дальнейшего использования и восстановления исходной информации.

5. Оценка надежности групповой схемы разделения данных и линейной. Из алгоритма построения кода в системе остаточных классов (СОК) следуют свойства остатков a_i, представляющих операнд A_k: независимость, равноправность и малоразрядность. Рассмотрим, как влияют эти свойства на структуру ЭВМ и математическую модель ее надежности [12].

независимость остатков. Это дает возможность построения ЭВМ в виде набора (по числу оснований СОК) информационно независимых трактов, работающих параллельно во времени. При построении ЭВМ вычислительная система в СОК обладает модульностью конструкции, что позволяет осуществлять ремонт и техническое обслуживание, не прерывая решения задач. Для осуществления профилактических мероприятий не требуется высококвалифицированного обслуживающего персонала. Кроме этого ошибки, возникшие в тракте по основанию p_i не «размножаются» в остальные тракты ЭВМ; при этом безразлично имела ли место по этому основанию p_i однократная или многократная ошибка, или даже пачка ошибок длиной не более p_{i-1} двоичных разрядов. Таким образом, ошибка, возникшая в произвольном p_i тракте ЭВМ в СОК либо сохранится в этом тракте до конца вычислений, либо в процессе дальнейших вычислений самоустранится (например, если после возникшего сбоя в остатке α_i промежуточный результат умножится на число имеющее нулевую цифру по основанию p_i). В этом случае посредством СОК можно построить систему исправления ошибок при введении минимальной избыточности, использующую динамику вычислительного процесса, введя понятия альтернативной совокупности. Совокупность основания СОК p_{i1}, p_{i2}, …, p_{ik}, по которым числа $A_1, A_2, ..., A_k$, отличаются от неправильного операнда A, называется альтернативной совокупностью числа A и обозначается $W(A)$. Основная идея определения ошибочного остатка $\alpha_i = \alpha_i + \Delta\alpha_i$ состоит в том, что для получаемой в результате операции последовательности неправильных операндов $A_i\,(i = \overline{1,\rho})$ в динамике вычислительного процесса, не прерывая решения задачи, последовательно во времени определяются условные альтернативные совокупности $W(A) = W_{i-1}(A) \wedge W_i(A)$.За определенное время условные альтернативные совокупности стягиваются к ошибочному основанию (либо к двум основаниям p_i и p_n). После этого известными методами проводится коррекция искаженного остатка α_i. Отличительной особенностью данного метода коррекции ошибок является возможность исправления ошибки без останова вычислений, что важно для ЭВМ, функционирующие в реальном масштабе времени.

Детальное исследование рассматриваемой особенности СОК позволяет сделать вывод о том, что устройства, функционирующие в классе вычетов, относятся к легко контролируемым и легко диагностируемым объектам. Отмеченная особенность ЭВМ, функционирующей в СОК, способствует разработке эффективных методов контроля и диагностики.

♦ равноправность остатков. Любой остаток α_i числа A_k в СОК несет информацию обо всем исходном числе, что дает возможность чисто программными методами заменить искаженный тракт по модулю p_j на исправный (контрольный)

тракт по модулю m_i не прерывая решения задачи. СОК с двумя контрольными основаниями позволяет полностью сохранить работоспособность ЭВМ при отказах любых двух рабочих трактов. При возникновении третьего или даже четвертого отказов ЭВМ все еще может выполнять программу при некотором уменьшении точности или скорости вычислений, т.е. ЭВМ в СОК является исключительно «живучей», приближаясь в этом плане к живым организмам. Отметим, что данная особенность обуславливает одно из самых замечательных свойств СОК: одна и та же ЭВМ может иметь различную надежность при решении различных задач в зависимости от требований, предъявляемых к точности, объему памяти и быстродействию машины при их решении, т.е. в процессе решения различных задач на ЭВМ в СОК возможно осуществление «обменных» операций между точностью, быстродействием и надежностью.

♦ малоразрядность остатков. Эта особенность СОК позволяет эффективно применять табличные методы реализации арифметических операций. В этом случае большинство арифметических операций производится в один такт, что резко повышает быстродействие выполнения рациональных операций. Одновременно, табличные методы выполнения арифметических операций позволяют создать на базе матричных схем, высоконадежные вычислительные устройства.

В работе были сравнены надежность групповой и линейной схемы разделения данных. Расчёт надёжности представляет собой процедуру определения значений показателей надежности объекта с использованием методов, основанных на их вычислении по справочным данным о надежности элементов объекта, по данным о надежности объектов-аналогов, данным о свойствах материалов и другой информации, имеющейся к моменту расчета.

Вероятность того, что в системе, состоящей из n одинаковых и равно надёжных элементов, безотказно работают не менее k элементов, может быть вычислена по формуле:

$$P(t) = \sum_{i=k}^{n} \binom{n}{i} p(t)^i q(n)^{n-1}, \qquad (5)$$

где $p(t)$ – вероятность безотказной работы одного элемента системы; $q(t) = 1 - p(t)$; $\binom{n}{i} = \frac{n!}{k!(n-k)!}$ – биноминальный коэффициент из n по k.

Рассмотрим пример для вычисления надежности функции при $n = 5$, а $k = 3$. В качестве времени распределения безотказной работы одного элемента системы применим экспоненциальный закон распределения $p(t) = \lambda e^{-\lambda t}$ при $\lambda = 1$. Тогда подставим значение в формулу (5) получим:

$$P(t) = \sum_{i=3}^{n} \frac{5!}{i!(5-i)!} (\lambda e^{-\lambda t})^i (1 - \lambda e^{-\lambda t})^{5-i}.$$

Так же рассмотрим вероятность безотказной работы системы при пропорциональном увеличении информационных и контрольных модулей, $n_x = 25$ а $k_x = 25$ тогда:

$$P_x(t) = \sum_{i=15}^{25} \frac{25!}{i!(25-i)!} (\lambda e^{-\lambda t})^i (1 - \lambda e^{-\lambda t})^{25-i}.$$

На рис. 8 показаны графики зависимости времени безотказной работы системы $P(t)$ и $P_x(x)$.

Из графика видно, что время работы системы $P_x(x)$ намного меньше, чем $P(t)$.

Проинтегрировав $P(t)$ и $P_x(x)$ получим среднее время безотказной работы системы: $\int_0^\infty P(t)dt = 0.783$, $\int_0^\infty P_x(t)dt = 0.564$. Следовательно, при пропорциональном увеличении информационных и контрольных модулей надежность системы падает. Для рассмотренного нами примера снижение среднего времени работы системы составляет 72 %.

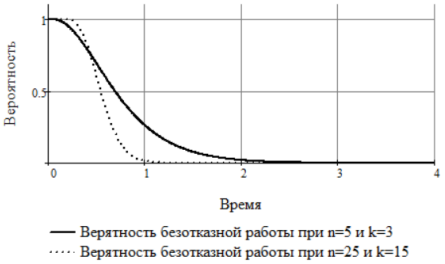

Рис. 8. Графики безотказной работы систем $P(t)$ и $P_x(x)$

Далее рассмотрим пример для определения среднего времени работы схемы с групповым разделением данных. Для этого разобьем схему из 25 элементов на 5 групп по 5 частей. В каждой группе 2 элемента будут избыточны и 2 группы будут избыточны. Тогда вероятность безотказной работы любой группы может быть оценена как

$$P_g(t) = \sum_{i=3}^{5} \frac{5!}{i!(5-i)!} (\lambda e^{-\lambda t})^i (1-\lambda e^{-\lambda t})^{n-i},$$

а системы в целом

$$P_{ob}(t) = \sum_{i=3}^{5} \frac{5!}{i!(5-i)!} (P_g(t))^i (1-P_g(t))^{n-i}.$$

На рис. 9 показаны графики зависимости времени безотказной работы системы $P_{ob}(t)$ и $P_x(t)$.

Из графика видно, что время работы системы групповой схемы разделения сданных $P_{ob}(t)$ выше, чем линейной $P_x(t)$.

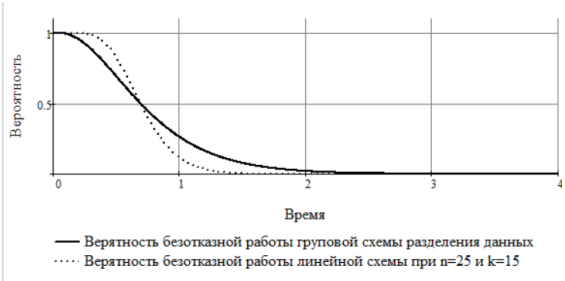

Рис. 9. графики безотказной работы систем $P_{ob}(t)$ и $P_x(t)$

Проинтегрировав $P_{ob}(t)$ и $P_x(t)$ получим среднее время безотказной работы системы: $\int_0^\infty P_{ob}(t)dt = 0.719$, $\int_0^\infty P_x(t)dt = 0.564$. Следовательно, при одинаковом числе участников схемы обмена сообщениями целесообразно использование групповой схемы разделение данных. Для рассмотренного нами примера преимущество групповой схемы составляет 78%.

Заключение. Рассмотренный метод разделения информации на группы подмножеств основанный на СОК показал, что его обнаруживающая способность кода составляет $\left(\frac{p_{n1}-p_{k1}}{p_{n1}}+\frac{p_{n2}-p_{k2}}{p_{n2}}+...+\frac{p_{nm}-p_{km}}{p_{nm}}\right)+\frac{p_n-p_k}{p_n}$ в отличие от классического $\frac{p_n-p_k}{p_n}=\frac{p_n-1}{p_n}$. Также уменьшение разрядности частей информации приведет к снижению нагрузки на сети передачи данных, либо сервера.

Рассмотрены способы восстановления информации из СОК в ПСС. Оценка надежности показала, что среднее время работы групповой схемы разделения информации выше, на рассмотренных нами примерах она увеличивается на 78%.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Kaya K., Selçuk A.A.* Robust Threshold Schemes Based on the Chinese Remainder Theorem // Progress in Cryptology – AFRICACRYPT 2008. – Springer, Berlin, Heidelberg, 2008. – P. 94-108.
2. *Iftene S.* General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting // Electron. Notes Theor. Comput. Sci. – 2007. – Vol. 186. – P. 67-84.
3. *Krasnobaev V. et al.* The Formulation and Solution of the Task of the Optimum Reservation in the System of Residual Classes // 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). – 2019. – P. 1-4.
4. *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. – М.: Советское радио, 1968. – 440 р.
5. *Goldreich O., Ron D., Sudan M.* Chinese remaindering with errors // IEEE Transactions on Information Theory. – 2000. – Vol. 46, No. 4. – P. 1330-1338.
6. *Mignotte M.* How to Share a Secret // Cryptography. – Springer, Berlin, Heidelberg, 1982. – P. 371-375.
7. *Asmuth C., Bloom J. A* modular approach to key safeguarding // IEEE Transactions on Information Theory. – 1983. – Vol. 29, No. 2. – P. 208-210.
8. *Чмора А.Л.* Современная прикладная криптография: учеб. пособие. – М.: Гелиос АРВ, 2001. – 256 р.
9. *Червяков Н.И., Кочеров Ю.Н., Евдокимов А.А.* Управление ресурсами распределенной вычислительной системы на базе группового протокола разделения секрета. – Уфа: УГНТУ, 2013. – Р. 163-168.
10. *Кочеров Юрий Николаевич, Червяков Николай Иванович.* Модификация схемы разделения данных Асмута-Блума с применением Метода Фрактальной Геометрии // Инфокоммуникационные технологии. – 2017. – Т. 15, № 1. – С. 7-14.
11. *Garner H.L.* The Residue Number System // Papers Presented at the the March 3-5, 1959, Western Joint Computer Conference. – New York, NY, USA: ACM, 1959. – P. 146-153.
12. *Kuzmenko I.* et al. Modification of the Scheme of Division of Asmuth-Bloom Data with the Application of the Method of Fractal Geometry // 2017 IVth International Conference on Engineering and Telecommunication (EnT). – 2017. – P. 28-32.
13. *Sorin Iftene, Ioana Boureanu.* Weighted Threshold Secret Sharing Based on the Chinese Remainder Theorem // Sci. Ann. Cuza Univ. – 2015. – P. 161-172.
14. *Сахнюк П. и др.* Модулярные параллельные вычислительные структуры нейропроцессорных систем. – М.: Физматлит, 2003. – 288 р.

15. *Червяков, Н.И. et al.* Нейрокомпьютеры в остаточных классах. – М.: Радиотехника, 2003. – 272 p.
16. *Kocherov Y.N., Samoylenko D.V., Tikhonov E.E.* Modeling of Parallel Data Encryption Algorithms // 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon). – 2019. – P. 1-5.
17. *Червяков Николай Иванович и др*. Нейронная сеть с пороговой (k, t) структурой для преобразования остаточного кода в двоичный позиционный код: pat. 2380751 USA. – 2008.
18. *Червяков Н. и др.* Применение искусственных нейронных сетей и системы остаточных классов в криптографии. – М.: Физматлит, 2012. – 280 p.
19. *Kocherov Y.N., Samoylenko D.V., Tikhonov E.E.* Safe Storage of Biometric Data // 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon). – 2020. – P. 1-5.
20. *Kocherov Y.N., Samoylenko D.V., Koldaev A.I.* Development of an Antinoise Method of Data Sharing Based on the Application of a Two-Step-Up System of Residual Classes // 2018 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon). – 2018. – P. 1-5.

REFERENCES

1. *Kaya K., Selçuk A.A.* Robust Threshold Schemes Based on the Chinese Remainder Theorem, *Progress in Cryptology – AFRICACRYPT 2008.* Springer, Berlin, Heidelberg, 2008, pp. 94-108.
2. *Iftene S.* General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting, *Electron. Notes Theor. Comput. Sci*., 2007, Vol. 186, pp. 67-84.
3. *Krasnobaev V. et al.* The Formulation and Solution of the Task of the Optimum Reservation in the System of Residual Classes, *2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT),* 2019, pp. 1-4.
4. *Akushskiy I.Ya., Yuditskiy D.I.* Mashinnaya arifmetika v ostatochnykh klassakh [Machine arithmetic in residual classes]. Moscow: Sovetskoe radio, 1968, 440 p.
5. *Goldreich O., Ron D., Sudan M.* Chinese remaindering with errors, *IEEE Transactions on Information Theor*y, 2000, Vol. 46, No. 4, pp. 1330-1338.
6. *Mignotte M.* How to Share a Secret, *Cryptography*. Springer, Berlin, Heidelberg, 1982, pp. 371-375.
7. *Asmuth C., Bloom J. A* modular approach to key safeguarding, *IEEE Transactions on Information Theory*, 1983, Vol. 29, No. 2, pp. 208-210.
8. *Chmora A.L.* Sovremennaya prikladnaya kriptografiya: ucheb. posobie [Modern applied cryptography: textbook]. Moscow: Gelios ARV, 2001, 256 p.
9. *Chervyakov N.I., Kocherov Yu.N., Evdokimov A.A.* Upravlenie resursami raspredelennoy vychislitel'noy sistemy na baze gruppovogo protokola razdeleniya sekreta [Resource management of a distributed computing system based on a group secret sharing protocol]. Ufa: UGNTU, 2013, pp. 163-168.
10. *Kocherov Yuriy Nikolaevich, Chervyakov Nikolay Ivanovich.* Modifikatsiya skhemy razdeleniya dannykh Asmuta-Bluma s primeneniem Metoda Fraktal'noy Geometrii [Modification of the Asmut-Bloom data separation scheme using the Fractal Geometry Method], *Infokommunikatsionnye tekhnologii* [Infocommunication technologies], 2017, Vol. 15, No. 1, pp. 7-14.
11. *Garner H.L.* The Residue Number System, *Papers Presented at the the March 3-5, 1959, Western Joint Computer Conference*. New York, NY, USA: ACM, 1959, pp. 146-153.
12. *Kuzmenko I.* et al. Modification of the Scheme of Division of Asmuth-Bloom Data with the Application of the Method of Fractal Geometry, *2017 IVth International Conference on Engineering and Telecommunication (EnT)*, 2017, pp. 28-32.
13. *Sorin Iftene, Ioana Boureanu.* Weighted Threshold Secret Sharing Based on the Chinese Remainder Theorem, *Sci. Ann. Cuza Univ*., 2015, pp. 161-172.
14. *Sakhnyuk P. i dr.* Modulyarnye parallel'nye vychislitel'nye struktury neyroprotsessornykh system [Modular parallel computing structures of neuroprocessor systems]. Moscow: Fizmatlit, 2003, 288 p.
15. *Chervyakov, N.I. et al.* Neyrokomp'yutery v ostatochnykh klassakh [Neurocomputers in residual classes]. Moscow: Radiotekhnika, 2003, 272 p.

16. *Kocherov Y.N., Samoylenko D.V., Tikhonov E.E.* Modeling of Parallel Data Encryption Algorithms, *2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, 2019, pp. 1-5.
17. *Chervyakov Nikolay Ivanovich i dr*. Neyronnaya set' s porogovoy (k, t) strukturoy dlya preobrazovaniya ostatochnogo koda v dvoichnyy pozitsionnyy kod [Neural network with threshold (k, t) structure for converting residual code into binary positional code]: pat. 2380751 USA, 2008.
18. *Chervyakov N. i dr*. Primenenie iskusstvennykh neyronnykh setey i sistemy ostatochnykh klassov v kriptografii [Application of artificial neural networks and systems of residual classes in cryptography]. Moscow: Fizmatlit, 2012, 280 p.
19. *Kocherov Y.N., Samoylenko D.V., Tikhonov E.E.* Safe Storage of Biometric Data, *2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, 2020, pp. 1-5.
20. *Kocherov Y.N., Samoylenko D.V., Koldaev A.I.* Development of an Antinoise Method of Data Sharing Based on the Application of a Two-Step-Up System of Residual Classes, *2018 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, 2018, pp. 1-5.

Статью рекомендовал к опубликованию к.т.н. А.А. Евдокимов.

Кочеров Юрий Николаевич – Невинномысский технологический институт; e-mail: kocherov_yra@mail.ru; г. Невинномысск, Россия; тел.: 88655471776; к.т.н.; доцент базовой кафедры регионального индустриального парка.

Самойленко Дмитрий Владимирович – e-mail: 151082@mail.ru; ст. преподаватель кафедры информационных систем, электропривода и автоматики.

Kocherov Yuri Nikolaevich – Nevinnomyssk Technological Institute; e-mail: kocherov_yra@mail.ru; Nevinnomyssk, Russia; phone: +78655471776; cand. of eng. sc.; associate professor of the base department of the Regional Industrial Park.

Samoilenko Dmitry Vladimirovich – e-mail: 151082@mail.ru; art. lecturer at the department of information systems, electric drive and automation.

УДК 681.3 004.2 629.05 DOI 10.18522/2311-3103-2021-1-235-247

С.М. Соколов, Н.Д. Беклемишев, А.А. Богуславский

ОРГАНИЗАЦИЯ ЦЕЛЕНАПРАВЛЕННЫХ ПЕРЕМЕЩЕНИЙ ПОДВИЖНЫХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ЗРИТЕЛЬНЫХ ОРИЕНТИРОВ

Рассматривается решение навигационной задачи с помощью системы технического зрения, определяющей положение подвижного средства относительно ориентиров, указанных в окружающем пространстве. Навигация по ориентирам является наиболее объективным критерием расположения подвижного средства в окружающем пространстве. Способ измерения параметров соотношений, характеризующих расположение подвижного средства относительно ориентиров, является почти независимым от других навигационных измерений. Ввод данных для корректировки координат и других параметров движения может производится не непрерывно, а в некоторые дискретные, и, в общем случае, довольно редкие моменты времени. Рассматривается общая схема решения: от постановки, до получения навигационной информации. Кратко описывается комплексирование полученных данных с данными от других навигационных средств, анализируются ключевые проблемы и параметры СТЗ, влияющие на точность получаемых результатов. Ключевым моментом в рассматриваемом способе является решение системы уравнений, описывающих положение робототехнических комплексов относительно указанных ориентиров. Эта система решается модифицированным методом Гаусса-Ньютона для нелинейной переоп-