Разработка метода аутентификации для обеспечения информационной скрытности низкоорбитальной группировки космических аппаратов

И.А. Калмыков, Н.К. Чистоусов, А.Ф. Чипига, М.И. Калмыков, Д.Н. Павлюк

«Северо-Кавказский федеральный университет», Ставрополь, Россия

Аннотация: Применение систем опознавания космического аппарата позволяет повысить информационную скрытность низкоорбитальных группировок космических аппаратов (НГКА). Однако существующие методы опознавания «свой-чужой» не обеспечивают высокую криптостойкость, а протоколы аутентификации с нулевым разглашением требуют больших временных затрат. Устранить данный недостаток можно за счет использования кодов полиномиальной системы классов вычетов (ПСКВ), которые позволяют осуществлять параллельные вычисления в протоколе. Поэтому разработка высокоскоростного протокола аутентификации с нулем разглашением является актуальной задачей. Цель работы – снижение временных затрат необходимых на вычисление статуса спутника за счет применения кодов ПСКВ.
Ключевые слова: метод аутентификации, протокол аутентификации космического аппарата, код полиномиальной системы классов вычетов.

Введение

Повышенный интерес к низкоорбитальным группировкам космических аппаратов (далее НГКА) возник в результате разработки и внедрения глобальных проектов по освоению Крайнего Севера и Арктики. В первую очередь это обусловлено техническими характеристиками НГКА, которые способны предоставить обмен контента между абонентами, располагающимися в северных широтах. При реализации российского проекта «Сфера» будет разработана глобальная многофункциональная инфокоммуникационная спутниковая система, в которой, используя 640 низкоорбитальных спутников, пользователям, находящимся в районах Крайнего Севера и Арктики, будет предоставлен широкополосный доступ в интернет [1].

По мере увеличения низкоорбитальных группировок космических аппаратов будет возрастать вероятность возникновения возможности навязывания неавторизованного контента абонентам. Для предотвращения

данной угрозы предлагается использовать методы аутентификации на основе протоколов с нулевым разглашением для повышения информационной скрытности НГКА. Применение системы опознавания статуса спутника позволит предотвратить возможность навязывания ретрансляционных помех. Однако существующие методы аутентификации с нулевым разглашением требуют больших временных затрат. Устранить данный недостаток можно за счет использования кодов полиномиальной системы классов вычетов (далее ПСКВ), которые позволяют осуществлять параллельные вычисления [2,3]. Поэтому разработка высокоскоростного метода аутентификации с нулевым разглашением на базе кодов ПСКВ является актуальной задачей.

Цель исследования

Для снижения вероятности пропуска неавторизованного претендента в протоколах с нулевым разглашением процесс аутентификации выполняется многократно [4]. Устранить данный недостаток способен метод аутентификации, приведенный в работе [5], в котором процесс опознавания состоит из двух этапов. Повысить эффективность данного метода аутентификации, используемого в НГКА, можно за счет использования кодов ПСКВ. Характерной чертой кодов ПСКВ является параллельное выполнение модульных операций, что позволяет повысить скорость вычислений. Цель работы – снижение временных затрат на вычисление статуса спутника за счет применения кодов ПСКВ.

Материалы и методы

Одним из способов, позволяющим обеспечить информационную скрытность НГКА, является применение системы опознавания «свой-чужой». Проведенные исследования [6-8] показали, что известные такие системы нецелесообразно променять в НГКА. Для решения данной проблемы был проведен сравнительный анализ методов аутентификации. К первой группе,

согласно работе [4], относят методы аутентификации на основе паролей с использованием хеш-функции $h(pass\ P)$ и шифрованием $E_k(pass\ P)$

$$P \to V : \left(ind\ P, h(pass\ P)\right),\ P \to V : \left(ind\ P, E_k(pass\ P)\right),$$

где $ind\ P, pass\ P$ – идентификатор и пароль претендента P; V – проверяющая сторона.

Недостатком данных методов является низкая криптостойкость. Ко второй группе относятся методы аутентификации на основе «запрос-ответ» [4], использующие шифрование

$$1.\ V \to P : b_V;$$
$$2.\ P \to V : E_{k_{PV}}\left(ind\ P, b_V\right);$$

где k_{PV} – общий секретный ключ P и V; b_V – случайное число.

Недостатком этих методов является использование шифрования, требующее периодической замены секретных ключей, что обеспечить в НГКА достаточно сложно. Третью группу составляют методы, построенные на основе нулевого разглашения знаний [4]. Данные методы имеют высокую криптографическую сложность, но требуют многократного повторения раунда аутентификации. Устранить данный недостаток позволяет метод аутентификации, который показан в работе [5].

Входные данные: M – большое простое число, g – порождающий элемент, K – секретный ключ спутника, S, T – числа, используемые для получения сеансового ключа $S(j)$ и $T(j)$ для определения повторного применения $S(j)$.

Предварительные вычисления: Используя функции F_1, F_2 претендент вычисляет $S(j)$ и $T(j)$, а также истинный $C(j)$ и зашумленный $C^*(j)$ статусы.

$$1.\ P: S(j) = F_1\ (K, S),\ T(j) = F_2\ (K, S, T),\ \{K, S(j), T(j)\} < M;$$
$$2.\ P: C(j) = g^{\mathrm{K}} g^{S(j)} g^{T(j)} \bmod M;$$
$$3.\ P: \{\Delta K(j),\ \Delta S(j),\ \Delta T(j)\} < \varphi(M);$$
$$4.\ P: K^*(j) = \left|K + \Delta K(j)\right|^{+}_{\varphi(M)},\ S^*(j) = \left|S + \Delta S(j)\right|^{+}_{\varphi(M)},$$
$$T^*(j) = \left|T + \Delta T(j)\right|^{+}_{\varphi(M)};$$
$$5.\ P: C^*(j) = g^{\mathrm{K}^*} g^{S^*(j)} g^{T^*(j)} \bmod M$$

Тело протокола. Претендент P готовит три ответа на полученный вопрос-число $d(j)$, а после их передает запросчику вместе с истинным $C(j)$ и зашумленным $C^*(j)$ статусами.

$$6.\ V \to P: d(j) \le \varphi(M) - 2;$$
$$7.\ P: r_1\ (j) = \left|K^*(j) - d(j)K\right|^{+}_{\varphi(M)},\ r_2\ (j) = \left|S^*(j) - d(j)S(j)\right|^{+}_{\varphi(M)},$$
$$r_3\ (j) = \left|T^*(j) - d(j)T(j)\right|^{+}_{\varphi(M)};$$
$$8.\ P \to V: \{C(j), C^*(j), r_1\ (j)\ r_2\ (j)\ r_3\ (j)\}.$$

Проверяющая сторона V выполняет проверку ответов и сравнивает со статусом $C^*(j)$. После генерирует сигнал «свой» или «чужой».

$$9.\ V: Y(j) = (C(j))^{d(j)} g^{r_1(j)} g^{r_2(j)} g^{r_3(j)} \bmod M;$$
$$10.\ V: \begin{cases} "свой", & если\ Y(j) = C^*(j); \\ "чужой", & если\ Y(j) \ne C^*(j). \end{cases}$$

Недостаток данного метода – низкая скорость выполнения мультипликативных операций из-за большой разрядности числа M. Устранить данный недостаток возможно за счет применения в данном протоколе аутентификации кодов ПСКВ.

Для получения кодов ПСКВ выбираются неприводимые многочлены конечных полей $p_i(x)$, где, произведение которых определяет разрядность диапазона кода [9,10]

$$\deg P(x) = \deg \prod_{i=1}^{k} p_i\ (x).$$

Тогда код ПСКВ для полинома $M(x)$, где $\deg M(x) < \deg P(x)$, имеет вид

$$M(x) = (M_1(x), M_2(x), ..., M_k(x)),$$

где $M_i(x) \equiv M(x) \bmod p_i(x)$, $i = 1, 2, ..., k$.

Коды ПСКВ позволяют эффективно выполнять модульные операции,

$$M(x) + C(x) = \left|M_1(x) + C_1(x)\right|^+_{p_1(x)}, ..., \left|M_k(x) + C_k(x)\right|^+_{p_k(x)},$$

$$M(x) \cdot C(x) = \left|M_1(x) \cdot C_1(x)\right|^+_{p_1(x)}, ..., \left|M_k(x) \cdot C_k(x)\right|^+_{p_k(x)},$$

где $\deg C(x) < \deg P(x)$; $C_i(x) \equiv C(x) \bmod p_i(x)$; $i = 1, 2, ..., k$.

Рассмотрим разработанный метод аутентификации с использованием протокола с нулевым разглашением знаний, реализованный в ПСКВ. Входные данные: набор оснований кода ПСКВ $p_1(x), ..., p_k(x)$, разрядность диапазона кода $\deg P(x)$, K – секретный ключ спутника, S, T – числа, используемые для получения сеансового ключа $S(j)$ и параметра $T(j)$ для определения повторного применения $S(j)$, удовлетворяющие $\log_2\{K, S(j), T(j)\} < \deg P(x)$. Выходные данные: сигнал «свой», сигнал «чужой».

Предварительные вычисления: Используя псевдослучайные функции F_1 и F_2, претендент P вычисляет $S(j)$ и $T(j)$, которые разбиваются на блоки по $\deg p_i(x)$ бит для вычисления истинного $C(j)$ и зашумленного $C^*(j)$ статусов.

$$\begin{aligned} &1.\ P: S(j) = F_1(K, S),\ T(j) = F_2(K, S, T),\ \log_2\{K, S(j), T(j)\} < \deg P(x); \\ &P: K = (K_1 \,||\, ... \,||\, K_k),\ S(j) = (S_1(j) \,||\, ... \,||\, S_k(j)),\ T^j = (T_1(j) \,||\, | \,||\, ... \,||\, T_k(j)); \end{aligned} \quad (1)$$

$$2.\ P: C(j) = \begin{cases} g^{K_1} g^{S_1(j)} g^{T_1(j)} \bmod p_1(x), \\ ... \\ g^{K_k} g^{S_k(j)} g^{T_k(j)} \bmod p_k(x), \end{cases} \quad (2)$$

$$3.\ P:\left\{\Delta K_i(j),\Delta S_i(j),\Delta T_i(j)\right\}<\deg p_i(x);L=2^{\deg p_i(x)}-1,$$
$$4.\ P:K_i^*(j)=\left|K+\Delta K_i(j)\right|_L^+,S_i^*(j)=\left|S_i(j)+\Delta S_i(j)\right|_L^+,$$
$$T_i^*(j)=\left|T_i(j)+\Delta T_i(j)\right|_L^+; \qquad (3)$$
$$5.\ P:C^*(j)=\begin{cases}g^{K_1^*}g^{S_1^*(j)}g^{T_1^*(j)}\bmod p_1(x),\\ \ldots\\ g^{K_k^*}g^{S_k^*(j)}g^{T_k^*(j)}\bmod p_k(x),\end{cases}$$

Тело протокола. Претендент P готовит три ответа на полученный вопрос-число $d(j)$, а после их передает запросчику вместе с истинным $C(j)$ и зашумленным $C^*(j)$ статусами.

$$6.\ V\to P:\log_2 d(j)<\deg P(x);d(j)=d_1(j)\|d_2(j)\|\ldots\|d_k(j);$$
$$7.\ P:r_i^W(j)=\left|K_i^*(j)-d_i(j)K_i\right|_L^+,r_i^W(j)=\left|S_i^*(j)-d_i(j)S_i(j)\right|_L^+,$$
$$r_i^W(j)=\left|T_i^*(j)-d_i(j)T_i(j)\right|_{L)}^+;W=1,2,3;L=2^{\deg p_i(x)-1}; \qquad (4)$$
$$8.\ P\to V:\left\{C_i(j),C_i^*(j),r_i^W(j)\,r_i^W(j)\,r_i^W(j)\right\}.$$

Проверяющая сторона V выполняет проверку ответов и сравнивает со статусом $C^*(j)$. После генерирует сигнал «свой» или «чужой».

$$9.\ V:Y_i(j)=(C_i(j))^{d_i(j)}g^{r_i^W(j)}g^{r_i^W(j)}g^{r_i^W(j)}\bmod p_i(x);$$
$$10.\ V:\begin{cases}"свой", & если\ Y_i(j)=C_i^*(j);\\ "чужой", & если\ Y_i(j)\neq C_i^*(j).\end{cases} \qquad (5)$$

Результаты исследования и обсуждение

Пусть $p_1(x)=x^5+x^2+1$, $p_2(x)=x^5+x^3+x^2+x+1$, $p_3(x)=x^5+x^3+1$ основания ПСКВ, которые задают диапазон $P(x)=\prod_{i=1}^{3}p_i(x)=x^{15}+x^7+x^3+x+1$.

1.Пусть секретный ключ $K=4236=0010000100\,01100_2$, параметры $S(j)=F_1(K,S)=15001$, $T(j)=F_2(K,S,T)=10867$, $\log_2\{K,S(j),T(j)\}<15$. По формуле (1) разобьем их на блоки по 5 бит каждый.

$$K = (K_1 \,||\, K_2 \,||\, K_3) = (00100 \,||\, 00100 \,||\, 01100) = (4 \,||\, 4 \,||\, 12),$$
$$S(j) = (S_1(j) \,||\, S_2(j) \,||\, S_3(j)) = (01110 \,||\, 10100 \,||\, 11001) = (14 \,||\, 20 \,||\, 25),$$
$$T(j) = (T_1(j) \,||\, T_2(j) \,||\, T_3(j)) = (01010 \,||\, 10011 \,||\, 10011) = (10 \,||\, 19 \,||\, 19).$$

2. Ответчик определяет истинный статус по выражению (2)

$$C(j) = \begin{cases} g^{K_1} g^{S_1(j)} g^{T_1(j)} \bmod p_1(x) = \left| x^4 \cdot x^{14} \cdot x^{10} \right|^{+}_{x^5+x^2+1} = \left| x^{28} \right|^{+}_{x^5+x^2+1} = x^4 + x^2 + x, \\ g^{K_2} g^{S_2(j)} g^{T_2(j)} \bmod p_2(x) = \left| x^4 \cdot x^{20} \cdot x^{19} \right|^{+}_{x^5+x^3+x^2+x+1} = \left| x^{12} \right|^{+}_{x^5+x^3+x^2+x+1} = x+1, \\ g^{K_3} g^{S_3(j)} g^{T_3(j)} \bmod p_3(x) = \left| x^{12} \cdot x^{25} \cdot x^{19} \right|^{+}_{x^5+x^3+1} = \left| x^{25} \right|^{+}_{x^5+x^3+1} = x^4 + 1. \end{cases}$$

3. Ответчик выбирает случайные числа, удовлетворяющие условию (3)

$$\Delta K(j) = (\Delta K_1(j) \,||\, \Delta K_2(j) \,||\, \Delta K_3(j)) = (01101 \,||\, 11001 \,||\, 11011) = (13 \,||\, 25 \,||\, 27),$$
$$\Delta S_i(j) = (\Delta S_1(j) \,||\, \Delta S_2(j) \,||\, \Delta S_3(j)) = (00110 \,||\, 10100 \,||\, 00001) = (6 \,||\, 20 \,||\, 1),$$
$$\Delta T_i(j) = (\Delta T_1(j) \,||\, \Delta T_2(j) \,||\, \Delta T_3(j)) = (00011 \,||\, 01011 \,||\, 01111) = (3 \,||\, 11 \,||\, 15).$$

4. Ответчик определяет зашумление параметров протокола

$$K^*(j) = \left(\left| K_1 + \Delta K_1(j) \right|^{+}_{31}, \left| K_2 + \Delta K_2(j) \right|^{+}_{31}, \left| K_3 + \Delta K_3(j) \right|^{+}_{31} \right) = (17 \,||\, 29 \,||\, 8),$$
$$S^*(j) = \left(\left| S_1(j) + \Delta S_1(j) \right|^{+}_{31}, \left| S_2(j) + \Delta S_2(j) \right|^{+}_{31}, \left| S_3(j) + \Delta S_3(j) \right|^{+}_{31} \right) = (20 \,||\, 9 \,||\, 26),$$
$$T^*(j) = \left(\left| T_1(j) + \Delta T_1(j) \right|^{+}_{31}, \left| T_2(j) + \Delta T_2(j) \right|^{+}_{31}, \left| T_3(j) + \Delta T_3(j) \right|^{+}_{31} \right) = (13 \,||\, 30 \,||\, 3).$$

5. Ответчик определяет зашумленный статус на основе кодов ПСКВ

$$C^*(j) = \begin{cases} \left| g^{K_1^*} g^{S_1^*(j)} g^{T_1^*(j)} \right|^{+}_{p_1(x)} = \left| x^{17} \cdot x^{20} \cdot x^{13} \right|^{+}_{p_1(x)} = \left| x^{19} \right|^{+}_{x^5+x^2+1} = x^2 + x, \\ \left| g^{K_2^*} g^{S_2^*(j)} g^{T_2^*(j)} \right|^{+}_{p_2(x)} = \left| x^{29} \cdot x^{9} \cdot x^{30} \right|^{+}_{p_2(x)} = \left| x^{6} \right|^{+}_{p_2(x)} = x^4 + x^3 + x^2 + x, \\ \left| g^{K_3^*} g^{S_3^*(j)} g^{T_3^*(j)} \right|^{+}_{p_3(x)} = \left| x^{8} \cdot x^{26} \cdot x^{3} \right|^{+}_{p_3(x)} = \left| x^{6} \right|^{+}_{x^5+x^3+1} = x^4 + x. \end{cases}$$

6. Запросчик передает $d(j) = 9561 = (d_1(j) \,||\, d_2(j) \,||\, d_3(j)) = (9 \,||\, 10 \,||\, 25)$.

7. Ответчик спутника готовит три ответа на полученный вопрос *d(j)*

$$r^1(j)=\left(\left|17-9\cdot 4\right|_{31}^{+},\left|29-10\cdot 4\right|_{31}^{+},\left|8-25\cdot 12\right|_{31}^{+}\right)=(12\,||\,20\,||\,18),$$
$$r^2(j)=\left(\left|20-9\cdot 14\right|_{31}^{+},\left|9-10\cdot 20\right|_{31}^{+},\left|26-25\cdot 25\right|_{31}^{+}\right)=(18\,||\,26\,||\,21),$$
$$r^3(j)=\left(\left|13-9\cdot 10\right|_{31}^{+},\left|30-10\cdot 19\right|_{31}^{+},\left|3-25\cdot 19\right|_{31}^{+}\right)=(16\,||\,26\,||\,24).$$

8. Ответчик передает истинный, зашумленный статусы и ответы по (4).

9. Запросчик осуществляет проверку статуса спутника согласно (5)

$$Y_1\ (j)=\left|(x^4+x^2+x)^4\cdot x^{12}\cdot x^{18}\cdot x^{16}\right|_{x^5+x^2+1}^{+}=x^2+x,$$

$$Y_2\ (j)=\left|(x+1)^{10}\cdot x^{20}\cdot x^{26}\cdot x^{26}\right|_{x^5+x^3+x^2+x+1}^{+}=x^4+x^3+x^2+x,$$

$$Y_3\ (j)=\left|(x^4+x)^{25}\cdot x^{21}\cdot x^{18}\cdot x^{24}\right|_{x^5+x^3+1}^{+}=x^4+x.$$

Так как $Y_1\ (j)=C_1^*(j), Y_2\ (j)=C_2^*(j), Y_3\ (j)=C_3^*(j)$, то выходной сигнал системы опознавания «свой». Спутник может установить связь с абонентом.

Программная реализация предложенного метода аутентификации была выполнена с использованием технологии Compute Unified Device Architecture (далее CUDA) в среде Matlab 2018. В результате этого были использованы графические процессоры на видеокарте NVidia GeForce 1050Ti с тактовой частотой 1290 МГц, что позволило осуществить параллельную обработку данных. Разрядность обрабатываемых данных в одномодульном протоколе составила 128 бит. В разработанном протоколе было выбрано восемь 16-разрядных неприводимых полинома. При использовании одномильного метода аутентификации временные затраты на определение статуса претендента составили 0,819 мкс. Реализация разработанного метода аутентификации времени потребовала 0,202 мкс. Таким образом, применение разработанного метода аутентификации, реализованного в ПСКВ, позволило сократить временные затраты в 4,05 раза по сравнению с одномодульным протоколом.

Выводы

В статье рассмотрены вопросы реализации протоколов аутентификации с нулевым разглашением знаний с использованием кодов полиномиальной системы классов вычетов. Показано, что за счет распараллеливания арифметических операций коды ПСКВ позволяют повысить скорость вычислений. На основе кодов ПСКВ был разработан метод аутентификации космического аппарата, позволяющий обеспечить информационную скрытность низкоорбитальной группировки космических аппаратов. Была разработана программная реализация метода аутентификации в ПСКВ с использованием технологии CUDA в среде Matlab 2018. В результате этого были использованы графические процессоры на видеокарте NVidia GeForce 1050Ti с тактовой частотой 1290 МГц. Проведенные исследования показали, что при использовании восьми 16-разрядных неприводимых полиномов реализация разработанного метода аутентификации времени потребовала 0,202 мкс, что в 4,05 раза по сравнению с одномодульным протоколом.

Литература

1. Спутниковая система глобальной связи или Глобальная многофункциональная информационная спутниковая система. // URL: tadviser.ru/index.php/ (дата обращения: 20.04.2020).

2. Ananda Mohan Residue Number Systems. Theory and Applications. Bangalore: Springer International Publishing Switzerland, 2016. 353 с.

3. Черняков Н.И., Коляда А.А., Ляхов П.А. и др. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях. Москва: ФИЗМАТЛИТ, 2017. 400 с.

4. Запечников С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности . Москва: Горячая линия-Телеком, 2011. 256 с.

5. Пашинцев В.П., Ляхов А.В. Применение помехоустойчивого протокола аутентификации космического аппарата для низкоорбитальной системы спутниковой связи// Инфокоммуникационные технологии. 2015. № 2. С. 183-190.

6. Ivtsenkov G. Simplifying and cost-effective IR-RF combat identification friend-or-foe (IFF) system for ground targets // Protective Arms Systems Inc. (Burlington, Ontario, CA) //Patent 8.184.195, Document Identifier US 20100289691 A1, Nov 18, 2010

7. Roes John, Varshneya Deepak Secure covert combat identification friend-or-foe (IFF) system for the dismounted soldier// Cubic Defense Systems, Inc. (San Diego, CA) //Patent 8.184.195, Document Identifier US 20090058712 A1, Mar 5, 2009.

8. Kymissis; Ioannis (New York, NY) Friend or foe detection // The Trustees of Columbia University in the City of New York (New York, NY) // Patent 8,750,517, Document Identifier US 20100266126 A1, Jun 10, 2014

9. Горденко Д. В., Резеньков Д. Н., Саркисов А. Б. Методы и алгоритмы реконфигурации непозиционных вычислительных структур для обеспечения отказоустойчивости спецпроцессоров. Ставрополь: Издательство Фабула, 2014. 180 с.

10. Калмыков И.А. Емарлукова Я.В. Математические модели и схемные решения отказоустойчивых непозиционных вычислительных систем: Монография. Ставрополь: Изд-во СКФУ, 2016. 216 с.

References

1. Sputnikovaya sistema global’noy svyazi ili Global’naya mnogofunktsional’naya informatsionnaya sputnikovaya sistema. [Global Satellite System or Global Multifunctional Satellite Information System]. URL: tadviser.ru/index.php/

2. Ananda Mohan Residue Number Systems. Theory and Applications. Bangalore: Springer International Publishing Switzerland, 2016. 353 c.

3. Chervjakov N.I., Koljada A.A., Ljahov P.A. i dr. Modulyarnaya arifmetika i eye prilozheniya v infokommunikatsionnykh tekhnologiyakh. [Modular arithmetic and its applications in infocommunication technologies] Moskva: FIZMATLIT, 2017. 400 p.

4. Zapechnikov S. V. Kriptograficheskie protokoly i ih primenenie v finansovoj i kommercheskoj dejatel'nosti. [Cryptographic protocols and their application in the financial and commercial activities]. Moskva: Gorjachaja linija-Telekom, 2011. 256 p.

5. Pashincev V.P., Ljahov A.V. Primenenie pomehoustojchivogo protokola autentifikacii kosmicheskogo apparata dlja nizkoorbital'noj sistemy sputnikovoj svjazi.[Application of a noise-free spacecraft authentication protocol for a low-orbit satellite communications system]. Infocommunication Technologies. 2015. № 2. P. 183-190

6. Ivtsenkov G. Simplifying and cost-effective IR-RF combat identification friend-or-foe (IFF) system for ground targets. Protective Arms Systems Inc. (Burlington, Ontario, CA). Patent 8.184.195, Document Identifier US 20100289691 A1, Nov 18, 2010

7. Roes John, Varshneya Deepak Secure covert combat identification friend-or-foe (IFF) system for the dismounted soldier. Cubic Defense Systems, Inc. (San Diego, CA). Patent 8.184.195, Document Identifier US 20090058712 A1, Mar 5, 2009.

8. Kymissis; Ioannis (New York, NY) Friend or foe detection. The Trustees of Columbia University in the City of New York (New York, NY). Patent 8,750,517, Document Identifier US 20100266126 A1, Jun 10, 2014

9. Gordenko D. V., Rezen'kov D. N., Sarkisov A. B. Metody i algoritmy rekonfiguracii nepozicionnyh vychislitel'nyh struktur dlja obespechenija

otkazoustojchivosti specprocessorov. [Methods and algorithms for reconfiguring non-positional computing structures to ensure fault tolerance of special processors] Stavropol: Publisher Fabula, 2014. 180 p.

10. Kalmykov I.A. Emarlukova Ja.V. Matematicheskie modeli i shemnye reshenija otkazoustojchivyh nepozicionnyh vychislitel'nyh system [Mathematical models and circuit solutions of fault-tolerant non-positional computing systems]: Monograph, Stavropol: Publishing house NCFU, 2016. 216 p.