Елисеев Алексей Сергеевич – ФГАНУ НИИ "Спецвузавтоматика", г. Ростов-на-Дону; e-mail: alexey.meteorite@gmail.com, alexeliseev@bk.ru; 344065, г. Ростов-на-Дону, пер. Днепровский, 124/6, кв. 99; тел.: +79043418984; к.т.н.; старший научный сотрудник.

Тикиджи-Хамбурьян Анна Рубеновна – e-mail: azick9@gmail.com; 344000, г. Ростов-на-Дону, ул. Соколова, 64/89, кв. 7; тел.: +79888990248; инженер-программист.

Eliseev Alexey Sergeevich – FSASE SRI "Specvuzavtomatika", Rostov-on-Don; e-mail: alexey.meteorite@gmail.com, alexeliseev@bk.ru; 124/6, Dneprovskiy pr., app. 99, Rostov-on-Don, 344065, Russia; phone: +79043418984; cand. of eng. sc.; senior scientist.

Tikidzhi-Khamburian Anna Rubenovna – e-mail: azick9@gmail.com; 64/89, Sokolova street, app. 7, Rostov-on-Don, 344000, Russia; phone: +79888990248; engineer-programmer.

УДК 004.056

Ю.Е. Рябинин, О.А. Финько

УСТОЙЧИВАЯ К АТАКАМ СТЕГАНОГРАФИЧЕСКАЯ СИСТЕМА В РАСШИРЕННОМ МОДУЛЯРНОМ КОДЕ

Не имея возможности вскрыть передаваемые по стеганографическому каналу легальными пользователями сообщения, злоумышленник применяет атаки, разрушающие встроенные в стеганографический контейнер данные. Одним из возможных решений описанной проблемы является применение распределенной многоканальной системы обмена стеганографическими сообщениями в расширенном модулярном коде. Суть предлагаемой стеганографической системы заключается в представлении встраиваемых в стеганографические контейнеры сообщений (предварительно зашифрованных по известному алгоритму и ключу) наименьшими неотрицательными вычетами модулярного кода. Вычисляются избыточные символы модулярного кода. Это обеспечивает устойчивую передачу информации по стеганографическим каналам связи при деструктивных воздействиях злоумышленника в сетях общего пользования. Представлена оценка достоверности передаваемых данных, получены расчетные формулы для вычисления вероятностей возникновения ошибок. Достигнутые результаты позволяют проектировать стеганографические системы, устойчивые к возможным атакам, характерным для указанных систем и обеспечивающие высокую степень достоверности передаваемых шифрованных данных в сети общего пользования.

Модулярный код; стеганография; Китайская теорема об остатках; остаток; основание; достоверность.

Ju.E. Ryabinin, O.A. Finko

STEGANOGRAPHIC SYSTEM RESISTANT TO ATTACK IN THE EXTENDE MODULAR ARITHMETIC

Not being to open transmitted legitimate users by steganography channel from of the message, the attacker uses the attacks, destroying built-in steganographic the container data. One possible solution for the above problems is the use of distributed multi-channel system of exchange of steganographic messages in the extended modular code. The essence of the proposed steganographic system is to provide embedded in containers steganographic messages (pre- encrypted by a known algorithm and key) least nonnegative residue modular code. Calculated excess characters modular code. It provides a robust data transmission over steganography communication channels with the destructive effects attacker in public networks. Provides an assessment of the reliability of the transmitted data , obtained formulas for calculating the probability of errors. The achieved results allow for the design of steganographic systems, resistant to possible attacks, characteristic for these systems and ensure high reliability of the transmitted encrypted data within a public network.

Modular code; steganography; Chinese Remainder Theorem; remainder; basis; reliability.

Демаскирующие признаки шифрованного текста, передаваемого по каналам связи, повышают вероятность успешного осуществления атак криптоаналитика на передаваемую информацию. С решением данной проблемы позволяет справиться применение средств и методов стеганографии, которые, как известно, позволяют скрыть сам факт существования секретных данных при их передаче, хранении или обработке [1].

В свою очередь, считается, что злоумышленник обладает полным объемом знаний о стеганографии, а как следствие, выполняет регулярный поиск и осуществляет атаки на возможно действующие стеганографические системы (далее по тексту для краткости – стеганосистемы).

На рис. 1 в виде блок-схемы приведен порядок действий злоумышленника при стеганографическом анализе.

Рис. 1. Алгоритм действий злоумышленника при стеганографическом анализе

Известен ряд атак, направленных на стеганографический канал связи. Можно выделить следующие категории атак против таких систем [1, 2]:

- атаки против встроенного сообщения;
- атаки против стегодетектора;
- атаки против протокола использования сообщения;
- атаки против самого сообщения.

В описанной ситуации, обычные методы стеганографии не позволяют в полной мере защитить передаваемую информацию и контейнер от всех видов атак. Возможным решением здесь является применение методов и средств распределённой многоканальной передачи стегосообщений.

Анализ информационных источников в области распределенной обработки и передачи данных выявил перспективный метод, основанный на системе остаточных классов или, согласно других источников, модулярной арифметике [3]. Представление данных в модулярной арифметике называют модулярным кодом (МК).

Многоканальная стеганографическая система в модулярном коде. В МК любое число $0 \le C < P$, где $P = \prod_{i=1}^{k} p_i$ однозначно представляется последовательностью [4] $C = (c_1, c_2, \dots, c_k)_{\text{МК}}$, так что $c_i = C \mod p_i$; $i = 1, 2, , \dots, k$, а $p_1, p_2, \dots, p_k$ – попарно простые числа, называемыми основаниями системы. Числа c_i представляются любым способом.

На основании Китайской теоремы об остатках [4, 5] система вычетов

$$\begin{cases} C = c_1 \mod p_1, \\ C = c_2 \mod p_2, \\ \dots\dots\dots\dots\dots\dots, \\ C = c_k \mod p_k \end{cases} \quad (1)$$

имеет единственное решение C, если выполнены вышеуказанные условия.

Целое неотрицательное число $C < P$, где $P = \prod_{i=1}^{k} p_i$, представленное вычетами $c_1, c_2, \dots, c_k$ по системе попарно простых модулей $p_1 < p_2 < \dots < p_k$ может быть однозначно восстановлено посредством рекурсии [6]:

$$\begin{cases} h_1 = c_2, \\ h_2 = p_1(\delta_1(c_1 - h_1) \mod P_1) \mod P_1 + c_1, \\ h_3 = p_3(\delta_2(c_3 - h_2) \mod P_2) \mod P_2 + c_3, \\ h_4 = p_4(\delta_3(c_4 - h_3) \mod P_3) \mod P_3 + c_4, \\ \dots\dots\dots\dots\dots, \\ h_k = C = p_k(\delta_{k-1}(c_k - h_{k-1}) \mod P_{k-1}) \mod P_{k-1} + c_k, \end{cases}$$

где

$$P_1 = \prod_{i} p_2;$$

$$P_i = \prod_{j=1} p_j;$$

$$\delta_1 = (P_1 - p_1)^{-1} \mod P_1;$$

$$\delta_i = (P_i - p_{i+1})^{-1} \mod P_i.$$

Порядок функционирования предлагаемой стеганографической системы следующий. Сообщение M, передаваемое в сети общего пользования, зашифровывается в шифраторе по известному алгоритму (например, ГОСТ 28147-84) и ключу K. Оговоримся, что в статье не рассматривается метод шифрования, способ распространения и выбора ключей, предполагается, что ключи заданы.

Полученная криптограмма C_i в кодере МК, декомпозируется на числа (блоки, вычеты) c_i, подлежащие встраиванию в стеганографические контейнеры, таким образом, что $c_i = C_i \mod p_i$, $i = 1, 2, \dots, k$. Следовательно, криптограмма C_i представляется вектором $\vec{C}_i = [c_1\ c_2\ \dots\ c_k]$. В целях повышения достоверности передаваемой информации в условиях воздействия атак злоумышленником на стеганографический канал выполним операцию расширения полученного МК (РМК) путем введения избыточных оснований $p_{k+1}, \dots, p_{k+r}$ и получения избыточных вычетов $c_{k+1} = C_i \mod \text{p}_{k+1}, \dots, c_{k+r} = C_i \mod \text{p}_{k+r}$.

Будем предполагать, что

$$p_1 < p_2 < \dots < p_k < p_{k+1} < \dots < p_{k+r}. \quad (2)$$

Для восстановления числа C_i по $(c_1, c_2, \dots, c_{k+r})_{\text{МК}}$ не обязательно знать значения всех остатков c_i, $i = 1, 2, \dots, k + r$, а достаточно знания любых (учитывая условие (2)) j остатков [3]: $c_{i_1}, c_{i_2}, \dots, c_{i_j}$, где $i = 1, 2, \dots, k + r$, а $j = 1, 2, \dots,\ k + 1$.

Таким образом, представления криптограмм $\vec{C}_i = [c_1\ c_2\ \dots c_{k+1} \dots c_{k+r}]$ в РМК имеют r избыточных остатков, которые можно использовать для обнаружения и исправления ошибок в целях повышения верности передачи информации. Полученный РМК обнаруживает все одиночные ошибки, если $r \ge 1$, и исправляет одиночные ошибки, если $r \ge 2$ [4]. Под q-кратной ошибкой будем понимать произ-

вольное искажение q блоков c_i. Следовательно, в случае осуществления злоумышленником атак на $r-1$ переданных контейнеров получатель сможет полностью восстановить все переданное сообщение.

Далее, в стеганокодере по заданному алгоритму и ключу K_i выполняется встраивание блока c_i в контейнер T_i в соответствии со следующими зависимостями стеганографического преобразования в общем виде [1, 2]:

$$W = F(T, K, C);$$

$$C = D(W, K), \quad (3)$$

где T – множество контейнеров-оригиналов; C – множество секретных сообщений; K – множество секретных ключей; F, D – функции прямого и обратного стеганографических преобразований соответственно; W – множество контейнеров-результатов.

На рис. 2, в качестве примера, представлена блок-схема предлагаемой стеганографической системы с одним избыточным символом.

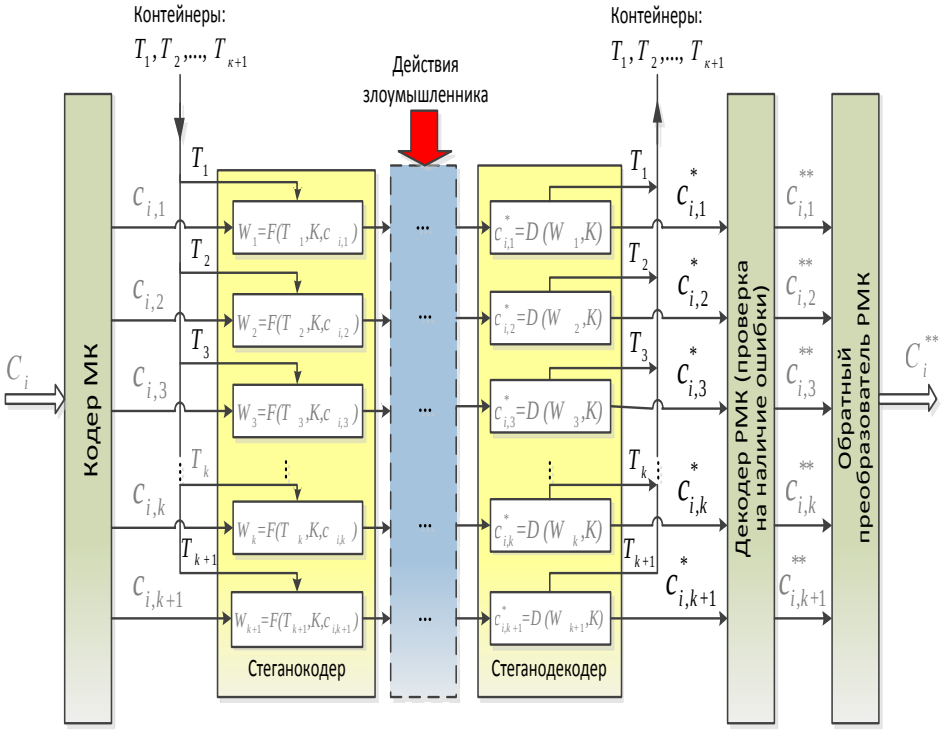

Рис. 2. Блок-схема стеганосистемы с обнаружением одиночных ошибок

На принимающей стороне получатель, приняв $k+r$ контейнеров по заданному алгоритму и ключу K в стеганодекодере, производит извлечение блока c_i из контейнера T_i в соответствии с зависимостью (3). Получив $k+r$ блоков и решив систему (1), в декодере РМК выполняется проверка на наличие ошибки в криптограмме по правилу [7]

$$C^*{}_i < P\,,$$

где $C^*{}_i$ – возможно содержащая ошибки криптограмма C_i.

Выполнение неравенства означает, что принятая последовательность не содержит обнаруживаемых ошибок. Если неравенство не выполнено, то регистрируется ошибка.

Таким образом, вводимая избыточность повышает устойчивость к атакам злоумышленника и увеличивает вероятность правильного приема переданной информации.

Оценка достоверности передаваемых данных. Оценим способность разработанной стеганосистемы верно передавать информацию в условиях деструктивных воздействий злоумышленника.

Учитывая способности кода в МА обнаруживать (исправлять) ошибки любой кратности в масштабе одного блока c_i, q-кратная ошибка определяется как произвольные искажения q символов вычета (блока). Примем, что искажение отдельных блоков происходит независимо друг от друга и подчиняются биноминальному закону распределения вероятностей. Искажение отдельных блоков есть совместные и независимые события. Пусть p – вероятность появления ошибки, тогда вероятность отсутствия ошибки $1-p$. Из вышесказанного, вероятность приема всех стеганоконтейнеров с ошибкой равна [8]

$$P = 1-(1-p)^n.$$

Используя формулу бинома Ньютона, получим

$$P(q) = \sum_{i=1}^{q} C_n^i (1-p)^{n-i} p^i . \qquad (4)$$

Таким образом, первый член разложения определяет вероятность одиночной ошибки – искажения q символов одного блока c_i, встроенного в стеганоконтейнер, второй – двукратной ошибки, т.е. искажение двух блоков c_i, а q-й – вероятности q-кратной ошибки. Отсюда

$$P(q) = \sum_{q=1}^{n} C_n^q (1-p)^{n-q} p^q,$$

где n – число блоков c_i (кодовых комбинаций), встроенных в стеганоконтейнеры.

Исходя из того, что модулярный код позволяет обнаруживать или исправлять часть искажений, очевидно, что не все ошибки приводят к неправильной регистрации кодовой комбинации на принимающей стороне. Искажения независимы и подчиняются биноминальному закону распределения. Тогда вероятность того, что кратность ошибки модулярного кода не превысит q искажений, определяется по формуле (4).

Если при передаче произойдут ошибки кратностью $q+1$ и выше, то такие ошибки уже не будут гарантированно обнаружены или исправлены. Следовательно, вероятность необнаруживаемых или неисправляемых ошибок, которая и определяет вероятность искажения блоков c_i МК, встроенных в стеганоконтейнеры, примет вид

$$P(q) = \sum_{i=q+1}^{n} C_n^i (1-p)^{n-i} p^i. \qquad (5)$$

Максимальное число достоверно исправляемых ошибок в кодовых комбинациях МК связано с кодовым расстоянием D_{min}.

Пусть $M = (m_1, \dots, m_2)_{\text{МК}}$ и $L = (l_1, \dots, l_2)_{\text{МК}}$ – представление чисел M и L в РМК. Назовем весом РМК числа M количество его ненулевых символов (остатков) и обозначим $\omega(M)$. Расстояние D между M и L определяется, как вес их разности $\omega(M-L)$. Для того, чтобы модулярный код исправлял q или менее ошибок необходимо и достаточно, чтобы минимальное кодовое расстояние кода D_{min}, удовле-

творяло условию: $D_{min} \geq 2q + 1$. Код с минимальным расстоянием D_{min} (здесь и далее - нечетное) гарантировано обнаруживает (исправляет) q ошибок [4]:

$$q_{\text{испр}} \leq \frac{D_{min} - 1}{2}, \quad q_{\text{обнар}} \leq D_{min} - 1\,. \tag{6}$$

Вводя в (5) параметр D_{min} и принимая во внимание связь между кодовым расстоянием и количеством исправляемых ошибок, описанную выражением (6), получаем следующие оценки для вероятности ошибочного декодирования при исправлении и обнаружении ошибок соответственно:

$$P_{\text{испр}}(q) \leq 1 - \sum_{q=0}^{\frac{D_{min}-1}{2}} C_n^q (1-p)^{n-q} p^q\,;$$

$$P_{\text{обнар}}(q) \leq 1 - \sum_{q=0}^{D_{min}-1} C_n^q (1-p)^{n-q} p^q.$$

Таким образом, получены расчетные формулы для вычисления вероятности возникновения необнаруживаемых и неисправляемых ошибок. Для сглаживания графических данных при проведении расчетов применим непрерывную гамма-функцию $\Gamma(n)$, $\Gamma(q)$. Расчеты будем выполнять по формуле

$$P(q) = \sum_{q=q+1}^{n} \frac{\Gamma(n+1)}{\Gamma(q+1)\Gamma(n-q+1)} (1-p)^{n-q} p^q.$$

На рис. 3 графически представлены расчетные данные зависимости вероятности недостоверного приема всей криптограммы от вероятности возникновения искажения стеганоконтейнера при передаче информации методами стеганографии со значениями $k = 12, r = 0$. Значение p изменяется на интервале от $1 \cdot 10^{-5}$ до 0,1.

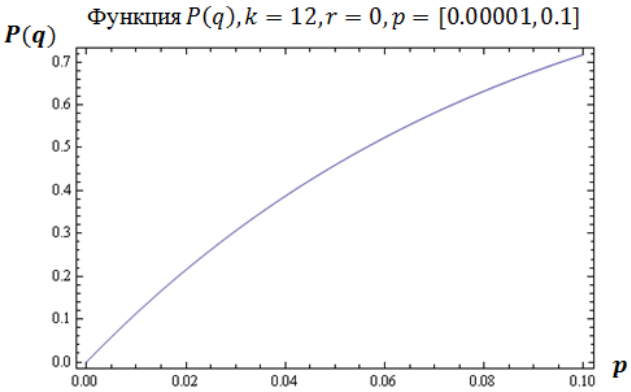

Рис. 3. Зависимость вероятности недостоверного приема всей криптограммы $P(q)$ от вероятности возникновения искажения стеганоконтейнера p при $r = 0$

На рис. 4–6 показано графическое представление расчетов с параметрами: $r = 1$, $r = 2$, $r = 3$, p изменяется на интервале от $1 \cdot 10^{-5}$ до $1 \cdot 10^{-4}$ и прежним значением k. Приведенные зависимости соответствуют стеганосистемам, обнаруживающим 1, 2 и 3-х кратные искажения соответственно.

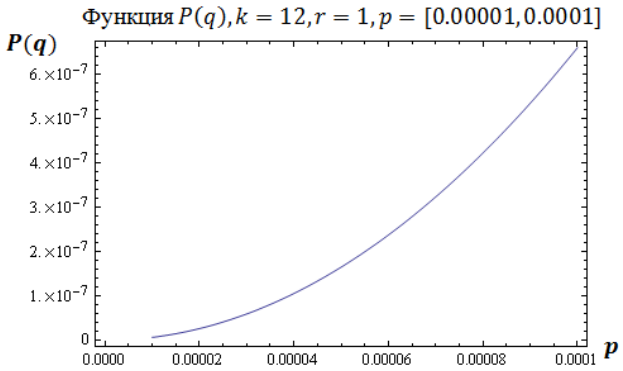

Рис. 4. Зависимость вероятности недостоверного приема всей криптограммы $P(q)$ от вероятности возникновения искажения стеганоконтейнера p при $r = 1$

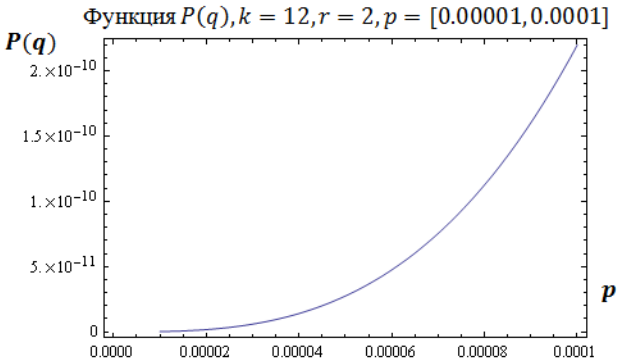

Рис. 5. Зависимость вероятности недостоверного приема всей криптограммы $P(q)$ от вероятности возникновения искажения стеганоконтейнера p при $r = 2$

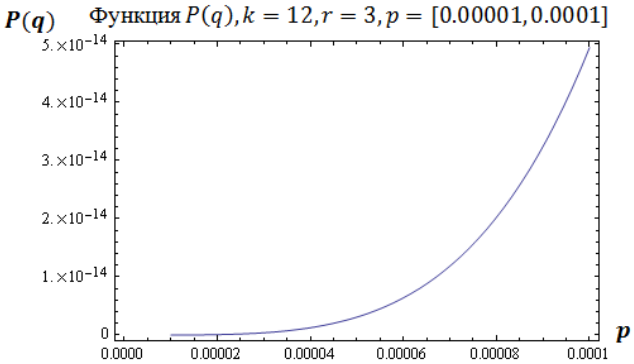

Рис. 6. Зависимость вероятности недостоверного приема всей криптограммы $P(q)$ от вероятности возникновения искажения стеганоконтейнера p при $r = 3$

Выводы. Разработанная стеганографическая система позволяет создать устойчивый скрытный канал обмена шифрованными данными в сети общего пользования, обеспечивающий высокую вероятность достоверной передачи шифрованной информации методами стеганографии.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Конахови Г.Ф., Пузыренко Ю.А.* Компьютерная стеганография: теория и практика. – Киев: МК-Пресс, 2006. – 283 с.
2. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография. – М.: Солон-Пресс, 2009. – 260 с.
3. *Самойленко Д.В., Финько О.А.* Имитоустойчивая передача данных в защищенных системах однонаправленной связи на основе полиномиальных классов // Нелинейный мир. – 2013. – Т.11, № 9. – С. 642-658.
4. *Бояринов И.М.* Помехоустойчивое кодирование числовой информации. – М.: Наука, 1983. – 196 с.
5. *Бухштаб А.А.* Теория чисел. – М.: Просвещение, 1966. – 384 с.
6. *Финько О.А.* Модулярная арифметика параллельных логических вычислений: Монография / Под ред. В.Д. Малюгина. – М.: ИПУ РАН, 2003. – 224 с.
7. *Акушский И.Я., Юдицкий Д.И.* Модулярная арифметика в остаточных классах. – М.: Сов. Радио, 1968. – 440 с.
8. *Гмурман В.Е.* Теория вероятности и математическая статистика. – М.: Высшая школа, 2003. – 480 с.

Статью рекомендовал к опубликованию д.т.н. В.Н. Марков.

Рябинин Юрий Евгеньевич – Филиал Военной академии связи (г. Краснодар); e-mail: jurandvau@inbox.ru; 350063, г. Краснодар, ул. Красина, 4; тел.: +79186218528; сотрудник.

Финько Олег Анатольевич – e-mail: ofinko@yandex.ru; тел.: +79615874848; кафедра криптографических средств защиты информации и математических основ криптологии; д.т.н.; профессор.

Ryabinin Jurii Evgenevich – Branch of the Military Academy of Communications (Krasnodar); e-mail: jurandvau@inbox.ru; 4, Krasina, Krasnodar, 350063, Russia; phone: +79186218528; employee.

Finko Oleg Anatolievich – e-mail: ofinko@yandex.ru; phone: +79615874848; the department of cryptographic protection of information and mathematical foundations of cryptology; dr. of eng. sc.; professor.

УДК 004.056 .55

Л.К. Бабенко, Д.А. Беспалов, О.Б. Макаревич, Р.Д. Чесноков, Я.А. Трубников

РАЗРАБОТКА И ИССЛЕДОВАНИЕ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ШИФРОВАНИЯ ПО АЛГОРИТМУ PRESENT ДЛЯ РЕШЕНИЯ ЗАДАЧ МАЛОРЕСУРСНОЙ КРИПТОГРАФИИ

Приведены результаты исследования одного из современных методов малоресурсной криптографии - блочного шифра PRESENT, а также некоторые практические результаты для программного решения и аппаратного модуля, выполненного в качестве отдельного устройства на базе программируемых логических интегральных схем (ПЛИС). Как показал анализ полученного решения, максимально допустимая частота работы схемы алгоритма для такой системы на кристалле определяется максимально допустимой частой тактирования ПЛИС и составляет 160 МГц, количество задействованных логических элементов составляет 297, количество задействованных блоков памяти – 0. Аппаратное решение алгоритма было выполнено для ПЛИС фирмы ALTERA Cyclone II EP2C20F484C7 с рабочими частотами 27, 50 и 100 МГц. Следует также упомянуть, что программное решение также адаптировано для технологии .NET Micro Framework и может применяться в 32- и 64-разрядных микроконтроллерах с архитектурой ARM7, ARM9 и Blackfin. Таким образом, получен ряд практически значимых результатов: проведено исследование алгоритма PRESENT, рассчитана трудоемкость, получено программное решение, достаточно эффективное для применения во встраиваемых устройствах, а также синтезирован аппаратный блок для системы на кристалле, удовлетворяющий всем требованиям малоресурсной криптографии, выполнена его