УДК 519.688

ПРИМЕНЕНИЕ МОДИФИКАЦИИ КРИПТОСИСТЕМЫ НИДЕРРАЙТЕРА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ВИДЕОИЗОБРАЖЕНИЙ

М. А. Самохина*,
ассистент,
Московский физико-технический институт

Рассматривается построение модификации криптосистемы Нидеррайтера, основанной на матрице фробениусовского вида, а также применение данной криптосистемы для передачи и защиты меняющихся изображений. Сделано заключение о криптостойкости системы.

Ключевые слова *— криптосистемы с открытым ключом, линейные коды, ранговые коды, криптоанализ, теория информации, защита информации, помехоустойчивое кодирование.*

Введение. Классическая криптосистема Нидеррайтера

В теории криптосистем с открытым ключом известны два основных типа систем, основанных на линейных кодах: система Мак Элиса (McElice) [1] и система Нидеррайтера [2]. В данной работе остановимся на криптосистемах, построенных на основе последней.

В качестве секретных ключей выбираются:

- проверочная матрица $\mathbf{H} = \left[z_j x_j^i \right]$, где $j = 1, 2, ..., n$, $i = 0, 1, ..., r - 1$, некоторого обобщенного кода Рида—Соломона над полем $GF(q)$;
- случайно выбранная невырожденная скремблирующая матрица $\mathbf{S}$ порядка r над полем $GF(q)$. Эта матрица вводится для того, чтобы скрыть от криптоаналитика видимые закономерности, разрушая структуру проверочной матрицы.

Открытым ключом является скремблированная проверочная матрица $\mathbf{H}_{cr} = \mathbf{SH}$.

Сообщениями являются все n-векторы с координатами из поля $GF(q)$ с весом, не превосходящим $r/2$. Здесь сообщения не являются кодовыми словами выбранного кода Рида—Соломона, а представляют собой всевозможные ошибки, которые этот код в состоянии исправлять.

Шифротекст, соответствующий сообщению m, представляет собой r-вектор и вычисляется следующим образом:

$$c = m\mathbf{H}_{cr}^T = m\mathbf{H}^T\mathbf{S}^T.$$

Законный пользователь после приема шифротекста c умножает его справа на матрицу $(\mathbf{ST})^{-1}$, а затем применяет известный лишь ему алгоритм быстрого декодирования и получает переданное сообщение m.

После официального представления данной классической схемы были предприняты неоднократные попытки ее вскрыть, которые увенчались успехом. В 1992 г. российскими криптоаналитиками Сидельниковым и Шестаковым была опубликована работа [3], где авторы описывали успешную атаку и приводили ее подробный алгоритм. Основная идея атаки состояла в раскрытии структуры закрытого ключа по открытому и подборе матриц $\tilde{\mathbf{H}}$ и $\tilde{\mathbf{S}}$ таких, что $\mathbf{H}_{cr} = \tilde{\mathbf{S}}\tilde{\mathbf{H}}$.

Новая модификация криптосистемы Нидеррайтера

В настоящее время существует три основных подхода к модификации криптосистемы. Первый подход заключается в зашумлении проверочной матрицы кода введением скрывающей матрицы. Например, в работе [4] была предложена скрывающая матрица единичного ранга. В работе [5] использовались скрывающие матрицы ранга, значительно большего единицы. Второй

*Научный руководитель — доктор техн. наук, профессор, заведующий кафедрой радиотехники Московского физико-технического института *Э. М. Габидулин*.

подход заключается в использовании различных метрик, отличных от классической хэммингова метрики. Например, выбирается ранговая метрика (как в работе [6]) или вводится некая новая метрика. И третий вариант модифицирования классической криптосистемы Нидеррайтера — это построение кодов с набором специфических свойств. Рассмотрим вариант применения сразу трех способов модификаций.

Модификация на основе фробениусовской метрики. Новая нехэмминговая метрика данной модификации строится на немодифицированной матрице Фробениуса. Выбирается некоторая матрица **F** фробениусовского вида размером $N \times n$ с элементами из поля $GF(q^N)$:

$$\mathbf{F} = \begin{pmatrix} h_1 h_1^q \ldots\ldots\ldots h_1^{q^{n-1}} \\ h_2 h_2^q \ldots\ldots\ldots h_2^{q^{n-1}} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ h_N \ldots\ldots h_N^q h_N^{q^{n-1}} \end{pmatrix}.$$

Каждый элемент матрицы — элемент расширенного поля $GF(q^N)$. Элементы $h_1, h_2, \ldots, h_N$ выбираются таким образом, чтобы они были линейно независимыми над ***базовым*** полем. Необходимо, чтобы ранг матрицы **F** не превосходил n и $n < N$. Обозначим $\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_N$ строки матрицы **F**. Норма любого ненулевого вектора **x** из пространства $GF(q^N)^n$ определяется как минимальное число ненулевых коэффициентов a_i в разложении:

$$\mathbf{x} = \sum_{i=1}^{n} a_i \mathbf{h}_i.$$

Для построения кода используется конкатенация матрицы **F** и некоторой матрицы $\mathbf{G}_k$, имеющей такую же структуру, как и **F**:

$$\mathbf{Q} = \begin{pmatrix} h_1 & h_1^q & \ldots & h_1^{q^{n-1}} \\ h_2 & h_2^q & \ldots & h_2^{q^{n-1}} \\ \vdots & \vdots & \ldots & \vdots \\ h_{N_1} & h_{N_1}^q & \ldots & h_{N_1}^{q^{n-1}} \\ g_1 & g_1^q & \ldots & g_1^{q^{n-1}} \\ g_2 & g_2^q & \ldots & g_2^{q^{n-1}} \\ \vdots & \vdots & \ldots & \vdots \\ g_K & g_K^q & \ldots & g_K^{q^{n-1}} \end{pmatrix} = \begin{pmatrix} \mathbf{F} \\ \mathbf{G}_k \end{pmatrix},$$

где

$$\mathbf{F} = \begin{pmatrix} h_1 & h_1^q & \ldots & h_1^{q^{n-1}} \\ h_2 & h_2^q & \ldots & h_2^{q^{n-1}} \\ \vdots & \vdots & \ldots & \vdots \\ h_{N1} & h_{N1}^q & \ldots & h_{N1}^{q^{n-1}} \end{pmatrix};$$

$$\mathbf{G}_k = \begin{pmatrix} g_1 & g_1^q & \ldots & g_1^{q^{n-1}} \\ g_2 & g_2^q & \ldots & g_2^{q^{n-1}} \\ \vdots & \vdots & \ldots & \vdots \\ g_k & g_k^q & \ldots & g_k^{q^{n-1}} \end{pmatrix};$$

$N_1 + K = N$; h_i, g_i — элементы поля $GF(q^N)$, линейно независимые в совокупности над базовым полем $GF(q)$. Верхняя часть матрицы **Q** с элементами $h_j^{q^i}$ используется для определения метрики, а нижняя часть с элементами $g_j^{q^i}$ используется как порождающая матрица кода.

При шифровании открытого текста $\mathbf{a} = (a_1 \quad a_2 \quad \ldots \quad a_k)$ из k информационных символов кодовый вектор вычисляется следующим образом:

$$\mathbf{y} = \mathbf{a}\mathbf{G}_k.$$

Вектор **y** можно представить в виде

$$\mathbf{y} = \Big(a_1 g_1 + a_2 g_2 + \ldots + a_k g_k \quad \ldots \quad a_1 g_1^{q^{n-1}} + a_2 g_2^{q^{n-1}} + \ldots + a_k g_k^{q^{n-1}}\Big),$$

где число ненулевых коэффициентов a_i равно s. Пусть вектор **y** имеет в новой метрике норму, равную $N_F = m$. Тогда **y** можно представить в виде

$$\mathbf{y} = \Big(b_b h_1 + b_2 h_2 + \ldots + b_m h_m \quad \ldots \quad b_1 h_1^{q^{n-1}} + b_2 h_2^{q^{n-1}} + \ldots + b_m h_m^{q^{n-1}}\Big).$$

Из полученных представлений вектора **y** следует, что $s + m$ строк матрицы **Q** линейно зависимы. Учитывая, что s и m натуральные и $s + m > n$, то $s + m \geq n + 1$ или $N_F \geq n - s + 1$.

Минимальное расстояние линейного кода равно минимальному весу ненулевых кодовых слов, поэтому минимальное расстояние рассматриваемого кода не будет превосходить N_F. Так как $k > s$, то $d_F \geq n - k + 1$. Учитывая обобщенную границу Синглтона, можно записать равенство $d_F = n - k + 1$.

Для удобства рассмотрения алгоритма расшифрования шифротекст можно представить в виде суммы

$$\mathbf{c} = \mathbf{g} + \mathbf{e},$$

где $\mathbf{g} = (g_1 \quad g_2 \quad \ldots \quad g_{N1})$ — кодовый вектор, а $\mathbf{e} = (e_1 \quad e_2 \quad \ldots \quad e_{N1})$ — вектор ошибки.

Пусть норма строки ошибки в новой метрике равна t, тогда вектор **e** представляется в виде

$$\mathbf{e} = m_1 h_1 + m_2 h_2 + \ldots + m_{N_1} h_{N_1},$$

причем

$$d_H(\mathbf{m}) = t.$$

Очень важно, что для кодов, описанных выше, существуют быстрые алгоритмы декодирования. При расшифровании легальный пользователь умножает полученный шифротекст $(\mathbf{g} + \mathbf{e})\mathbf{S}$ на $\mathbf{S}^{-1}$. Затем применяет алгоритм быстрого декодирования в новой метрике. В результате пользователь получит векторы $\mathbf{g}$ и $\mathbf{e}$ по отдельности. После применения алгоритма быстрого декодирования ***родительского кода*** легальный пользователь получит вектор $\tilde{\mathbf{m}}$. Далее для получения открытого текста m остается умножить $\tilde{\mathbf{m}}$ на P^{-1}.

Криптоанализ новой модификации криптосистемы Нидеррайтера

После построения криптосистемы необходимо рассмотреть применимость к ней ранее известных атак. В случае, если атака применима, нужно вычислить ее трудоемкость и сравнить с трудоемкостью атак на криптосистемы, признанные мировым сообществом стойкими на данный момент. По результатам сравнения можно сделать вывод о стойкости самой криптосистемы.

Можно выделить два основных вида атак, применимых к рассматриваемой криптосистеме, — прямые и структурные. Под прямыми атаками понимаются перебор по искусственным ошибкам, перебор по сообщениям, декодирование опубликованного кода как случайного. Структурные атаки — это различные модификации атаки Гибсона, адаптированные к изменениям в криптосистеме, а также вариант атаки Сидельникова—Шестакова. При оценке трудоемкости каждой из атак необходимо учитывать размер открытого ключа.

Криптоанализ рассматриваемой криптосистемы можно свести к двум основным этапам:

1) нахождение вектора-ошибки, который необходим для исправления ошибки в новой метрике;

2) вычисление открытого текста по синдрому.

Что касается первого пункта, то для него необходимо выполнить ряд трудоемких операций. Второй этап менее ресурсоемкий и частично реализован на примере атаки Сидельникова—Шестакова, тем не менее, вторая часть атаки бессмысленна без прохождения первого этапа.

Декодирование случайного кода в ранговой метрике сводится к решению параметрической системы квадратных уравнений в базовом поле [7]. Подход к решению такой системы включает в себя перебор по некоторым переменным полученной системы.

Таким образом построена атака на модификацию криптосистемы Нидеррайтера, основанную на фробениусовской метрике [8]. Общая трудоемкость наиболее сложной части процесса декодирования составляет порядка $O((Nr)^3 q^{(r-1)(k+1)-2})$. Количество неизвестных в решаемой системе равно $(k + m + 1) + N(r - 1)$. Таким образом, чтобы система была разрешима, необходимо, чтобы $(k + m + 1) + N(r - 1) \le mN$. Например, для (24, 12)-кода над полем $GF(2^{12})$, который может исправлять ошибки ранга вплоть до 3, сложность декодирования составит 2^{52}.

Опираясь на результаты проведенного криптоанализа, можно выделить основные условия для параметров криптосистемы, основанной на матрице Фробениуса, так, чтобы она могла считаться стойкой. При выборе (48, 24)-кода над полем $GF(2^{16})$ размер открытого ключа будет составлять 1 Кбит, а вычислительная сложность приведенной атаки составит порядка 2^{140}. Из данного примера видно, что для ключа в 1 Кбит (сегодня такой размер ключа используется во многих стандартных асимметричных криптосистемах) количество операций рассматриваемой структурной атаки велико. Таким образом, структурные атаки, даже специально модифицированные под криптосистему, основанную на фробениусовской метрике, нельзя назвать успешными.

Применение новой криптосистемы в качестве системы совместного исправления ошибок и защиты от несанкционированного доступа

Рассмотрим применение предлагаемой модификации криптосистемы Нидеррайтера в качестве системы совместного исправления ошибок и защиты от несанкционированного доступа. За счет того, что в криптосистеме используются коды, которые успешно применяются в помехоустойчивом кодировании, система может быть использована и как система, исправляющая ошибки канала.

Предположим, что при передаче зашифрованного сообщения в криптосистеме возникают различного рода помехи, что приводит к искажению кодового слова. В случае, когда присутствует ошибка канала $\tilde{\mathbf{e}}$, совпадающая с одним из базисных векторов, она имеет в новой метрике норму, равную 1. Если искусственная ошибка $\mathbf{e}$ имеет норму $t = (d - 3)/2$, тогда система может исправлять также и ошибки канала.

Чтобы гарантировать коррекцию ошибок канала, необходимо наложить дополнительные ограничения на выбор матриц в модуле инициализации. Для исправления ошибок канала в любом случае мы должны иметь представление о характере ошибок. Необходимо собрать статистику и, предварительно проанализировав ее, сделать вывод о характере ошибок и модификации криптосистемы в целях их исправления. В базовом поле шифротекст представляет собой матрицу с элементами из $GF(q)$

$$\mathbf{C} = \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{N1} & \cdots & c_{Nn} \end{pmatrix}.$$

Элементы матрицы **C** имеют вид

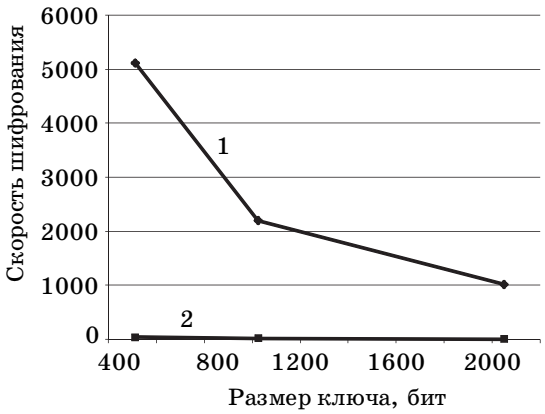
$$c_{ij} = \Big[s_{ij} \left(g_1 u_{1i} + \ldots + g_k u_{ki} + h_i \right) + \cdots + \\ + s_{jj} \left(g_1^{q^{j-1}} u_{1i} + \ldots + g_k^{q^{j-1}} u_{ki} + h_i^{q^{j-1}} \right) \Big] m_j.$$

Пусть приемник получил шифротекст, искаженный ошибкой, в виде $\mathbf{g} + \mathbf{e} + \tilde{\mathbf{e}}$. В таких случаях, для того чтобы гарантировать коррекцию ошибок канала, необходимо наложить дополнительные ограничения на выбор матрицы **Q**. В работе [9] подробно рассматриваются такие ограничения и их зависимость от вида ошибки канала. Дополнительные ограничения на выбор матрицы **Q** приводят к ухудшению криптосистемы с точки зрения ее криптостойкости, для увеличения стойкости системы в этом случае следует увеличивать размер ключа.

Применение криптосистемы для передачи и защиты меняющихся изображений

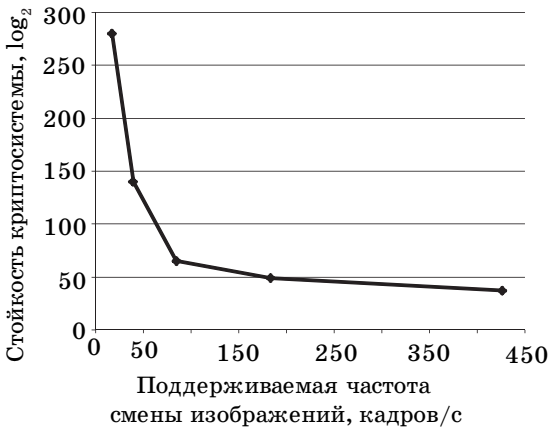
Новая модификация криптосистемы Нидеррайтера была предложена как часть новой системы с открытым ключом для передачи и защиты меняющихся изображений. При исследовании системы проводилось моделирование самой новой криптосистемы, системы сжатия видеоизображений и моделирование каналов с различного рода помехами. Автором данной статьи проводилось моделирование алгоритмов шифрования (и расшифрования) и согласование параметров системы в соответствии с существующими стандартами. Результаты исследования алгоритмов новой криптосистемы представлены на следующих графиках. На рис. 1 показана зависимость скорости шифрования от размера ключа криптосистемы для модифицированной системы Нидеррайтера, основанной на матрице Фробениуса, и криптосистемы RSA при размере ключа 512 бит в нешумящем канале. Из графика видно, что предлагаемая криптосистема оказывается быстрее, чем криптосистема RSA.

Значение поддерживаемой частоты для RSA в 2 раза ниже, чем аналогичное у предлагаемой новой криптосистемы. Такое сравнение не совсем корректно для шумящего канала, так как для использования RSA в шумящем канале необходимо производить кодирование с вероятностью ошибки в бите не более 10^{-8}. Это дополнительное ограничение на использование криптосистемы RSA, которое невозможно реализовать в случае канала с шумами, что приводит к дополнительным трудностям. Для их решения необходимы слишком ресурсоемкие затраты, такие как применение в дополнение к криптосистеме системы помехоустойчивого кодирования. В результате, кроме превосходства по скоростям, использование предлагаемой модификации криптосистемы Нидеррайтера не требует дополнительных затрат как для разработки программного комплекса, так и для увеличения вычислительных мощностей используемого аппаратного комплекса.

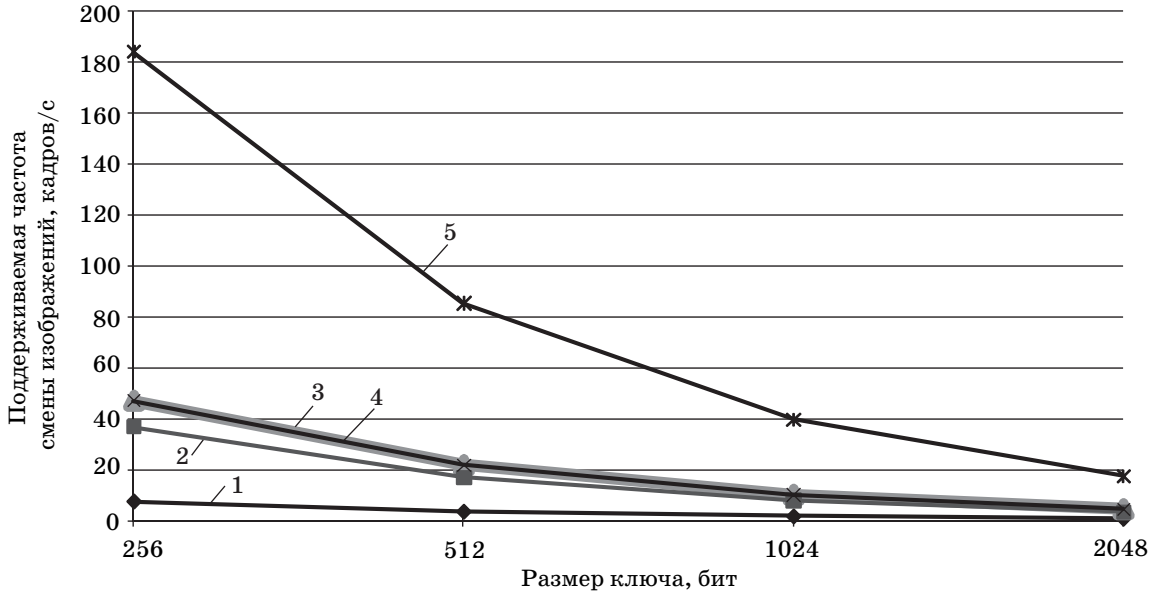


■ ***Рис. 1.*** *Зависимость скорости шифрования от размера ключа криптосистемы: 1 — модификация криптосистемы Нидеррайтера; 2 — RSA*

При различных параметрах криптосистемы ее стойкость будет варьироваться в зависимости от поддерживаемой частоты смены видеокадров. На рис. 2 представлен график такой зависимости в нешумящем канале при размере кадров, соответствующих возможностям сотового телефона SonyEricsson W900. Размер кадра при использовании современных методов сжатия составляет в среднем 12 Кбит (240 × 320 пикселей). Для ча-



■ ***Рис. 2.*** *Зависимость стойкости от поддерживаемой частоты смены кадров*



■ ***Рис. 3.*** *Зависимость частоты смены кадров от размера ключа: 1 — HDTV; 2 — видео стандартной четкости, SD; 3 — NTSC (National Television Standards Committee); 4 — сотовый телефон Nokia E66; 5 — сотовый телефон SonyEricsson W900*

стоты 25 кадров стойкость криптосистемы остается настолько высокой, что потери стойкости для исправления ошибок канала несущественны.

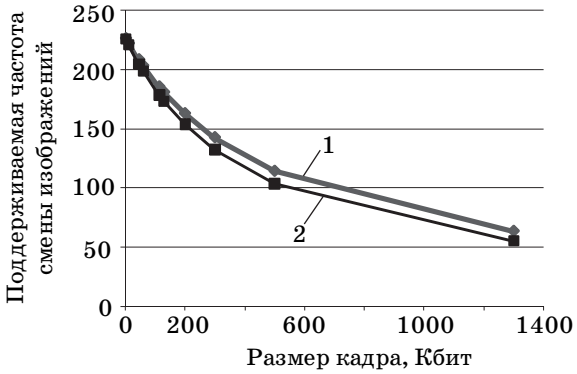
Далее рассмотрим результаты моделирования для размеров кадров, соответствующих различным стандартам. Графики зависимости поддерживаемой частоты смены кадров от размера ключа при различных размерах кадров при использовании модификации криптосистемы Нидеррайтера представлены на рис. 3.

Приведены средние значения размеров кадров для рассматриваемых стандартов и часто применяемых устройств, пиксель:

HDTV	1920 × 1080
Видео стандартной четкости, SD	720 × 576
NTSC	648 × 486
Сотовый телефон Nokia E66	640 × 480
Сотовый телефон SonyEricsson W990	240 × 320

В случае передачи видеоизображения повышенного качества HDTV частота смены изображений, поддерживаемой системой, заметно сокращается. Однако для видео стандартной четкости SD соответствующая этому стандарту частота в 25 кадров поддерживается и для канала с шумом.

Скорость шифрования в системе можно заметно увеличить, осуществляя шифрование изображения с помощью более производительных симметричных алгоритмов, а шифрование сеансового ключа осуществлять уже при помощи предлагаемой системы. Но такая модификация может быть применена только для случая канала без шума.



■ ***Рис. 4.*** *Зависимость частоты смены кадров от размера кадра: 1 — AES, теоретически возможный предел; 2 — AES*

Например, при использовании в качестве симметричного алгоритма AES или ГОСТ 28147–89 при выборе соответствующих параметров асимметричной криптосистемы можно уже гарантировать передачу изображения в формате стандарта HDTV.

Графики зависимости поддерживаемой частоты смены кадров от размера кадров при использовании симметричного алгоритма AES256 и новой модификации криптосистемы Нидеррайтера представлены на рис. 4. Размер сеансового ключа составляет 256 бит, размер открытого ключа системы — 512 бит.

Из графика видно, что даже при стандартной реализации AES без ускорений (линия *2*), поддерживаемая частота смены изображений возрастает в 10 раз.

Литература

1. **McElice R. J.** A Public Key Cryptosystem Based on Algebraic Coding Theory // DSN Progress Report 42-44. Pasadena, CA: Jet Propulsion Lab, 1978. P. 114–116.
2. **Niederreiter H.** Knapsack-Type Cryptosystem and Algebraic Coding Theory // Problem Control and Information Theory. 1986. Vol. 15. P. 19–34.
3. **Сидельников В. М., Шестаков С. О.** О системе шифрования, основанной на обобщенных кодах Рида—Соломона // Дискретная математика. 1992. Т. 3. Вып. 3.
4. **Gabidulin E., Ourivski A., Pavlouchkov V.** On the modified Niederreiter cryptosystem // Information Theory and Networking Workshop. Metsovo, Greece, 1999. P. 50.
5. **Габидулин Э. М., Обернихин В. А.** Коды в F-метрике Вандермонда и их применение. Долгопрудный: МФТИ, 2005.
6. **Габидулин Э. М.** Теория кодов с максимальным ранговым расстоянием // Проблемы передачи информации. Т. XXI. Вып. 1. 1985.
7. **Уривский А. В., Йоханссон Т.** Новые способы декодирования кодов в ранговой метрике и их криптографические приложения // Проблемы передачи информации. 2002. Т. 38. Вып. 3. С. 83–93.
8. **Самохина М. А.** Криптоанализ систем, основанных на линейных кодах // Проблемы информационной безопасности. Компьютерные системы. 2008. Вып. 2. С. 94–103.
9. **Самохина М. А.** Применение модификаций криптосистем Нидеррайтера в системах исправления ошибок и защиты от несанкционированного доступа // Моделирование и обработка информации: Сб. науч. тр. 2008. С. 127–136.

УВАЖАЕМЫЕ АВТОРЫ ЖУРНАЛА

При подготовке рукописей статей редакция просит Вас руководствоваться следующими рекомендациями.

Объем статьи (текст, таблицы, иллюстрации и библиография) не должен превышать эквивалента в 16 страниц, напечатанных на бумаге формата А4 на одной стороне через 1,5 интервала в Word шрифтом Times New Roman размером 13.

Обязательными элементами оформления статьи являются: индекс УДК, инициалы и фамилия автора (авторов), ученая степень, звание, полное название организации; заглавие, аннотация (5–7 строк) и ключевые слова на русском и английском языках.

Формулы набирайте в Word, при необходимости можно использовать формульный редактор; для набора одной формулы не используйте два редактора; при наборе формул в формульном редакторе знаки препинания, ограничивающие формулу, набирайте вместе с формулой; для установки размера шрифта никогда не пользуйтесь вкладкой Other..., используйте вкладку Define; в формулах не отделяйте пробелами знаки: + = –.

При наборе символов в тексте помните, что символы, обозначаемые латинскими буквами, набираются светлым курсивом, русскими и греческими — светлым прямым, векторы и матрицы — прямым полужирным шрифтом.

Иллюстрации в текст не заверстываются и предоставляются отдельными исходными файлами, поддающимися редактированию:

— рисунки, графики, диаграммы, блок-схемы изготавливаются в векторных программах: Visio 4, 5, 2002–2003 (*.vsd); Coreldraw (*.cdr); Excel; Word; AdobeIllustrator; AutoCad (*.dxf); Компас; Matlab (экспорт в формат *.ai);

— фото и растровые — в формате *.tif, *.png с максимальным разрешением (не менее 300 pixels/inch).

Наличие подрисуночных подписей обязательно (желательно не повторяющих дословно комментарии к рисункам в тексте статьи).

В редакцию предоставляются:

— сведения об авторе (фамилия, имя, отчество, место работы, должность, ученое звание, учебное заведение и год его окончания, ученая степень и год защиты диссертации, область научных интересов, количество научных публикаций, домашний и служебный адреса и телефоны, факс, e-mail), фото авторов: анфас, в темной одежде на белом фоне, должны быть видны плечи и грудь, высокая степень четкости изображения без теней и отблесков на лице, фото можно представить в электронном виде в формате *.tif, *.png с максимальным разрешением — не менее 300 pixels/inch при минимальном размере фото 40 × 55 мм;

— экспертное заключение.

Список литературы составляется по порядку ссылок в тексте и оформляется следующим образом:

— для книг и сборников — фамилия и инициалы авторов, полное название книги (сборника), город, издательство, год, общее количество страниц;

— для журнальных статей — фамилия и инициалы авторов, полное название статьи, название журнала, год издания, номер журнала, номера страниц;

— ссылки на иностранную литературу следует давать на языке оригинала без сокращений;

— при использовании web-материалов указывайте адрес сайта.