УДК 004.056.55

В. А. ЛИПНИЦКИЙ, С. И. СЕМЁНОВ

СИНДРОМНЫЕ СПЕКТРЫ ОРБИТ ОШИБОК В РС-КОДАХ

Военная академия Республики Беларусь, Минск, Республика Беларусь

Данная статья посвящена исследованию свойств синдромов ошибок в кодах Рида-Соломона. РС-коды построены на недвоичных алфавитах. Поэтому, в отличие от кодов Боуза-Чоудхури-Хоквингема, РС-коды содержат исключительно большое многообразие корректируемых ошибок. Для коррекции этих ошибок предлагается систематическое применение автоморфизмов кодов. Характерными автоморфизмами РС-кодов являются циклические и аффинные подстановки, образующие циклические группы Г и А соответственно, порядки которых совпадают с длиной кода. Показано, что циклическая и аффинная подстановки коммутируют друг с другом и порождают совместную АГ-группу как прямое произведение подгрупп А и Г. Данные три группы действуют на пространстве векторов-ошибок РС-кодов, разбивая это пространство на три вида орбит ошибок. Как правило, эти орбиты являются полными, то есть содержат максимально возможное количество ошибок. Синдромы являются основным индикатором наличия ошибок в каждом принятом ИКС сообщении, средством точной идентификации этих ошибок. Исследована специфика синдромов двойных ошибок в РС-кодах. Установлено, что спектры синдромов орбит ошибок также являются полными в подавляющем большинстве случаев. Доказано, что структура спектров синдромов копирует структуру самих орбит, которые в свою очередь копируют структуру групп автоморфизмов кода. Полученные результаты являются существенным вкладом в построение ТНС для кодов Рида-Соломона.

Ключевые слова: *линейный код, РС-код, синдромы ошибок, автоморфизмы кодов, циклическая подстановка, аффинная подстановка, орбиты векторов-ошибок.*

Введение

Коды Рида-Соломона, благодаря лежащему в их основе недвоичному алфавиту и большому минимальному расстоянию, способны корректировать большие ансамбли ошибок, поэтому постоянно расширяется спектр приложений данных кодов [1–3].

Перевод теории РС-кодов с полиномиального языка на матричный открывает перспективы широкого применения в обработке этих кодов теории поле Галуа, развития теории норм синдромов (ТНС) на коды Рида-Соломона [4, 5].

ТНС строится на основе хорошей, легко конструируемой группы автоморфизмов, действующих на применяемом линейном коде. В кодах БЧХ такими были циклические и циклотомические подстановки [5]. Как показали исследования [6], циклотомическая подстановка из-за недвоичного алфавита не может быть автоморфизмом РС-кода, однако при несколько расширенном понимании автоморфизма линейного кода (как невырожденного линейного преобразования) к ним можно отнести аффинные подстановки или гомотетии. Данная работа посвящена развитию существенного раздела ТНС – исследованию свойств синдромов ошибок и специфики синдромных спектров орбит ошибок в кодах Рида-Соломона.

Необходимые сведения о кодах Рида-Соломона

Под кодом Рида-Соломона мы понимаем линейный блоковый код длины $N = q–1$, определенный над полем Галуа $GF(q)$ из q элементов, где $q = p^m > 2$ для простого числа p и натуральное $m \geq 1$, который задается проверочной матрицей:

$$H = \left[\alpha^{bi}, \alpha^{(b+1)i}, \ldots, \alpha^{(\delta-2+b)i}\right]^T, \ 0 \leq i \leq N-1, \quad (1)$$

с элементами, принадлежащими полю $GF(q)$ [1, 3, 4]. Матрица (1) имеет размерность $(\delta–1)\times N$ и ранг $\delta–1$ над полем $GF(q)$. В дальнейшем этот код будем обозначать через $RS(N, K)$, где N – длина РС-кода, $K = N – \delta + 1$ – количество информационных символов, размерность кода. Минимальное расстояние РС-кода равно $D = N - K + 1 = \delta$ [1, с. 289].

На практике предпочтение отдается РС-кодам с $b = 1$. Тогда проверочная матрица (1) принимает вид:

$$H = \left[\alpha^i, \alpha^{2i}, \ldots, \alpha^{(\delta-1)i}\right]^T, \ 0 \le i \le N-1, \quad (2)$$

Векторы-ошибки в кодах $RS(N, K) = RS(q-1, q-\delta)$ принадлежат $(q-1)$-мерному векторному пространству $V_N(GF(q))$ над полем Галуа $GF(q)$. Поэтому в данном коде имеется всего $(q-1)^2$ ошибок весом 1; двойных – $C_{q-1}^2(q-1)^2$ ошибок весом $\omega \ge 1 - C_{q-1}^{\omega}(q-1)^{\omega}$, что в $(q-1)^{\omega}$ раз больше, чем у двоичного БЧХ-кода той же длины. Очевидно, с ростом N и ω количество исправляемых РС-кодом ошибок стремительно растёт, векторы-ошибки весом, меньшим D обнаруживаемы кодом $RS(N, K)$ и исправляемы, если их вес $t \le (D-1)/2$ для нечетных D и $t \le (D-2)/2$ для чётных значений D [1].

Понятие автоморфизмов в помехоустойчивом кодировании введено с сильной оглядкой на двоичные коды [1, глава 8]: это перестановки координат векторов, переводящие все кодовые слова в кодовые. В [6] доказано, что РС-код с проверочной матрицей (1) является циклическим потому, что оператор циклического сдвига σ, который действует на каждый вектор $\overline{e} = (e_1, e_2, \ldots, e_N) \in V_N(GF(q))$ по правилу: $\sigma(\overline{e}) = (e_N, e_1, e_2, \ldots, e_{N-1})$, кодовые слова кода $RS(N, K) = RS(q-1, q-\delta)$ преобразует в кодовые. Степени σ составляют циклическую группу $\Gamma = \{\sigma, \sigma^2, \ldots, \sigma^N = e\}$ порядка N для тождественного оператора e.

К принципиально иному типу автоморфизмов РС-кодов следует отнести аффинные подстановки или гомотетии, то есть преобразования $f_\gamma : \overline{x} \to \gamma\overline{x}$ векторного пространства $V_N(GF(q))$ – пространства ошибок кода $RS(N, K) = RS(q-1, q-\delta)$ [6].

Преобразования f_γ образуют группу А относительно операции композиции отображений, изоморфную циклической группе $GF(q)^*$ порядка q-1. В силу цикличности группа А имеет следующую структуру: А = $\langle f_\alpha \rangle = \{f_\alpha, f_{\alpha^2}, \ldots, f_{\alpha^N} = e\}$ для примитивного элемента α поля $GF(q)$, образующей мультипликативной группы $GF(q)^*$.

Не сложно проверить, что операторы f_γ и σ коммутируют друг с другом: $\sigma f_\chi = f_\chi \sigma$, что пересечение $\Gamma \cap \mathrm{A} = \{e\}$. Отсюда следует, что минимальная подгруппа в группе $Aut(RS(N, K))$ автоморфизмов РС-кода, содержащая А и Г, совпадает с их прямым произведением АГ и является группой порядка $(q-1)^2$.

Перечисленные автоморфизмы порождают три различных класса орбит векторов-ошибок в РС-кодах: А-орбиты, Г-орбиты и АГ-орбиты.

Для всякого вектора $\overline{e} \ne \overline{0}$ из пространства $V_N(GF(q))$ порожденная им А-орбита $\langle \overline{e} \rangle_{\mathrm{A}}$ имеет следующую структуру:

$$\langle \overline{e} \rangle_A = \left\{\overline{e}, f_\alpha(\overline{e}), f_{\alpha^2}(\overline{e}), \ldots, f_{\alpha^{N-1}}(\overline{e})\right\} =$$
$$\left\{\overline{e}, \alpha\overline{e}, \alpha^2\overline{e}, \ldots, \alpha^{N-1}\overline{e}\right\}.$$

Все А-орбиты, порожденные ненулевыми векторами, являются полными – содержат максимально возможное число векторов, имеют мощность N. Г-орбита $\langle \overline{e} \rangle_\Gamma$, порожденная этим же вектором, имеет похожую циклическую структуру:

$$\langle \overline{e} \rangle_\Gamma = \left\{\overline{e}, \sigma(\overline{e}), \sigma^2(\overline{e}), \ldots, \sigma^{N-1}(\overline{e})\right\},$$

где ν – наименьшее целое положительное число с условием: $\sigma^\nu(\overline{e}) = \overline{e}$. Когда $\nu = N$ Г-орбита также содержит максимально возможное количество векторов и потому является полной. Значение $\nu < N$ также возможно, реализуется, когда вес вектора является делителем числа N. К примеру, в пространстве $V_{15}(GF(2^4))$ вектор $\overline{e} = (\alpha, 0, 0, \alpha, 0, 0, \alpha, 0, 0, \alpha, 0, 0, \alpha, 0, 0)$ с примитивным элементом $\alpha \in GF(2^4)$ порождает, очевидно, Г-орбиту мощностью $\nu = 3$.

Каждая АГ-орбита $\langle \overline{e} \rangle_{\mathrm{A}\Gamma}$ состоит из $\nu(q-1)$ векторов для $\nu = N$ или для ν, делящего N, и, в силу взаимной коммутируемости подстановок σ и f_γ, имеет следующую структуру:

$$\langle \overline{e} \rangle_{\mathrm{A}\Gamma} = \left\{\langle \overline{e} \rangle_{\mathrm{A}}, \langle \sigma(\overline{e}) \rangle_{\mathrm{A}}, \ldots, \langle \sigma^{\nu-1}(\overline{e}) \rangle_{\mathrm{A}}\right\}$$

или

$$\langle \overline{e} \rangle_{\mathrm{A}\Gamma} = \left\{\langle \overline{e} \rangle_\Gamma, \langle (\alpha\overline{e}) \rangle_\Gamma, \ldots, (\alpha^{q-2}\overline{e}) >_\Gamma\right\}.$$

Таким образом, АГ-орбиту можно рассматривать как объединение N Г-орбит, переходящих друг в друга под действием автоморфизма f_α или же как объединение ν А-орбит.

Если K – множество всех корректируемых РС-кодом векторов-ошибок мощностью $|K|$, то оно разбивается на множество Г-орбит K_Γ или А-орбит K_{A}. Как правило, будем рассматривать наиболее крупные орбиты – АГ-орбиты. Подавляющее большинство АГ-орбит является полным – содержит по N^2 векторов-ошибок, поэтому мощность $|K_{АГ}|$ примерно равна величине $|K|/N^2$.

Спектры синдромов орбит ошибок в РС-кодах

Приемное устройство инфокоммуникационной системы (ИКС), работающее на основе РС-кода, проверяет каждое принятое сообщение $\overline{x}$ на наличие ошибок вычислением синдрома $S(\overline{x}) = H\overline{x}^T$. В соответствии со структурой проверочной матрицы (1) или (2) синдром представляет собой вектор $S(\overline{x}) = (s_1, s_2, \ldots, s_{\delta-1})$ с δ–1 координатами из поля $GF(q)$. Синдром $S(\overline{x})$ может быть любым вектором δ–1-мерного пространства над полем $GF(q)$. Таким образом, в РС-коде имеется $q^{\delta-1}$ различных синдромов векторов-ошибок. Если $S(\overline{x}) = 0$, то $\overline{x} = \overline{c}$ – правильное кодовое сообщение. Если же $S(\overline{x}) \neq 0$, то $\overline{x} = \overline{c} + \overline{e}$, где $\overline{e}$ – наложившийся на правильное сообщение $\overline{c}$ ненулевой вектор ошибок, подлежащий дальнейшей идентификации.

Из-за большого разнообразия спектра синдромов у РС-кодов некоторые привычные для двоичных БЧХ-кодов свойства синдромов здесь могут нарушиться. К примеру, у двоичных кодов Хемминга и БЧХ-кодов первая компонента синдрома любой двойной ошибки всегда отлична от нуля. У кодов же $RS(N, K)$ с проверочной матрицей (1) или (2) всегда найдутся примеры векторов-ошибок $\overline{e}$ весом 2 и с компонентой $s_1 = 0$ у синдрома $S(\overline{e}) = (s_1, s_2, \ldots, s_{\delta-1})$.

Более того, для каждого целого i, $1 \le i \le \delta–1$, найдётся вектор $\overline{e_i}$ весом 2 с компонентой синдрома $s_i = 0$. Например, вектор-ошибка $\overline{e_i} = \left(\alpha^i, 0, \ldots, 0, 1, 0, \ldots, 0\right)$ с 1 на i+1-ом месте в коде $RS(N, K)$ с проверочной матрицей (2). Однако, имеет место.

Лемма 1. В коде $RS(N, K)$ с проверочной матрицей (2) не существует векторов- ошибок весом 2, синдромы которых имели бы две компоненты, равные 0.

Доказательство методом от противного. Предположим, что такая вектор-ошибка $\overline{e}$ с компонентами $s_\mu = 0$, $s_\nu = 0$, $1 \le \mu < \nu \le \delta–1$, всё-таки существует $\overline{e} = (0, \ldots, 0, x, 0, \ldots, 0, y, 0, \ldots, 0)$ с неизвестными координатами $x,\ y \in GF(2^m)^*$ на неопределенных позициях i, j, $1 \le i < j \le N$. Компоненты s_μ и s_ν получаются умножением μ-ой и ν-ой строк матрицы (2) на вектор $\overline{e}$:

$$\begin{cases} s_\mu = \alpha^{(i-1)\mu}x + \alpha^{(j-1)\mu}y = 0; \\ s_\nu = \alpha^{(i-1)\nu}x + \alpha^{(j-1)\nu}y = 0. \end{cases} \quad (3)$$

Полученные равенства можно рассматривать как систему линейных однородных уравнений относительно неизвестных x и y. Определитель системы

$$\Delta = \alpha^{(i-1)\mu}\alpha^{(j-1)\nu} + \alpha^{(i-1)\nu}\alpha^{(j-1)\mu} = \alpha^{\nu(i-1)+\mu(j-1)}\left(1 + \alpha^{(\nu-\mu)(j-i)}\right) \neq 0.$$

По правилу Крамера данная система должна иметь единственное, а, следовательно, нулевое решение: $x = y = 0$. Но тогда вес вектора $\overline{e}$ равен нулю. Полученное противоречие завершает доказательство леммы.

Следствие 1. У синдрома любой двойной ошибки не менее δ–2 компонент отличны от нуля (все $s_i \neq 0$, за исключением, может быть, одной).

Конечно же, базовые свойства синдромов сохраняются и для РС-кодов. В том числе и такое свойство, как попарное различие синдромов у любой декодируемой совокупности векторов-ошибок, как например, попарное различие синдромов одиночных и двойных ошибок в РС-коде с проверочной матрицей (2).

Синдромы векторов-ошибок под действием на эти векторы автоморфизмов РС-кодов изменяются по строго определенным правилам.

Предложение 1.

Пусть $S(\overline{e}) = (s_1, s_2, \ldots, s_{\delta-1})^T$ – синдром вектора-ошибки $\overline{e}$ в РС-коде с проверочной матрицей (1). Тогда для автоморфизма циклического сдвига σ вектор $\sigma(\overline{e})$ имеет синдром

$$S\left(\sigma(e^-)\right) = (\alpha \wedge bs\_1, \alpha \wedge 2bs\_2, \ldots, \alpha \wedge (\delta-1)bs\_(\delta-1). \quad (4)$$

Если РС-код задан проверочной матрицей (2), то

$$S\left(\sigma(\overline{e})\right) = \left(\alpha s_1, \alpha^2 s_2, \ldots, \alpha^{\delta-1}s_{\delta-1}\right). \quad (5)$$

В РС-коде с проверочной матрицей (1) или (2) синдром

$$S\left(f_\gamma(\overline{e})\right) = (\gamma s_1, \gamma s_2, \ldots, \gamma s_{\delta-1}) = \gamma S(\overline{e}). \quad (6)$$

Доказательство. Пусть код задан проверочной матрицей (1). Пусть у вектора $\overline{e} = (e_1, e_2, \ldots, e_N)$

отличны от нуля координаты с номерами i_1, i_2, ..., i_s. Тогда для целого i, $1 \le i \le \delta-1$, компонента s_i синдрома $S(\overline{e}) = (s_1, s_2, \ldots, s_{\delta-1})^T$ является результатом умножения i-ой строки матрицы (1) на вектор $\overline{e}$ и есть величина

$$s_i = \alpha^{(b+i-1)(i_1-1)} e_{i_1} + \alpha^{(b+i-1)(i_2-1)} e_{i_2} + \ldots + \alpha^{(b+i-1)(i_s-1)} e_{i_s}.$$

У вектора $\sigma(\overline{e})$ ненулевыми будут координаты с номерами i_1+1, i_2+1, ..., i_s+1, соответственно равные $e_{i_1}, e_{i_2}, \ldots, e_{i_s}$. Поэтому у вектора $S(\sigma(\overline{e})) = (s_1^\sigma, s_2^\sigma, \ldots, s_{\delta-1}^\sigma)^T$ i-я компонента

$$s_i^\sigma = \alpha^{(b+i-1)i_1} e_{i_1} + \alpha^{(b+i-1)i_2} e_{i_2} + \ldots + \alpha^{(b+i-1)i_s} e_{i_s} = \alpha^{b+i-1}(\alpha^{(b+i-1)(i_1-1)} e_{i_1} + \alpha^{(b+i-1)(i_2-1)} e_{i_2} + \ldots + \alpha^{(b+i-1)(i_s-1)} e_{i_s}) = \alpha^{b+i-1} s_i,$$

что доказывает формулу (4). Формула (5) является частным случаем формулы (4). Формула (6) следует из свойств линейности синдрома и векторно-матричных вычислений: $S(\gamma\overline{e}) = \gamma S(\overline{e})$.

Следствие 1. Если у синдрома $S(\overline{e}) = (s_1, s_2, \ldots, s_{\delta-1})^T$ какая-нибудь из компонент $s_i = 0$ ($s_i \ne 0$), то этим же свойством обладают и все i-е компоненты всех векторов-ошибок из АГ-орбиты, которой принадлежит вектор $\overline{e}$.

Доказательство следствия непосредственно вытекает из формул (4)–(6).

Определение 1. Множество всех попарно различных синдромов каждой отдельно взятой орбиты векторов-ошибок называется синдромным спектром этой орбиты.

Формулы (4)–(6) показывают, что спектры синдромов каждой отдельно взятой Г-орбиты или А-орбиты имеют четко очерченную структуру, синхронно копирующую циклическую структуру самих орбит (для α – образующей группы $GF(2^m)^*$):

$$S(\langle\overline{e}\rangle_\Gamma) = \{\alpha^i s_1, \alpha^{2i} s_2, \ldots, \alpha^{(\delta-1)i} s_{\delta-1}\}, \quad 0 \le i \le \nu - 1, \nu = N \text{ или } \nu \text{ делит } N. \tag{7}$$

$$S(\langle\overline{e}\rangle_\mathrm{A}) = \{\alpha^i s_1, \alpha^i s_2, \ldots, \alpha^i s_{\delta-1}\}, 0 \le i \le N-1. \tag{8}$$

Предложение 2. Пусть код $RS(N, K)$ задан проверочной матрицей (2), а вектор-ошибка $\overline{e} \ne \overline{0}$, но и не является кодовым словом. Тогда А-орбита $\langle\overline{e}\rangle_\mathrm{A}$ является полной с полным спектром синдромов $S(\langle\overline{e}\rangle_\mathrm{A})$, то есть $|S(\langle\overline{e}\rangle_\mathrm{A})| = |\langle\overline{e}\rangle_\mathrm{A}| = N$.

Если Г-орбита $\langle\overline{e}\rangle_\Gamma$ имеет полный спектр синдромов (то есть мощность $|S(\langle\overline{e}\rangle_\Gamma)| = N$), то и Г-орбита $\langle\overline{e}\rangle_\Gamma$ является полной: $|\langle\overline{e}\rangle_\Gamma| = N$.

Пусть Г-орбита $\langle\overline{e}\rangle_\Gamma$ имеет мощность ν, равную N или делящую N, спектр синдромов которой также равен ν. Тогда орбита $\langle\overline{e}\rangle_{\mathrm{A}\Gamma}$ имеет мощность νN со спектром синдромов $S(\langle\overline{e}\rangle_{\mathrm{A}\Gamma})$ мощностью νN.

<u>Доказательство.</u> В условиях предложения 2 $S(\overline{e}) \ne \overline{0}$. А это означает, что по крайней мере одна из компонент $s_i \ne 0$ у синдрома $S(\overline{e})$. Тогда множество $\{\alpha^i \cdot s_i\}$, $0 \le j \le N-1$, имеет мощность N. В силу формулы (8) этот факт приводит к выводу, что спектр синдромов $S(\langle\overline{e}\rangle_\mathrm{A})$ также имеет мощность N.

Заключение

Синдромы являются основным индикатором наличия ошибок в каждом принятом ИКС сообщении, средством точной идентификации этих ошибок. Исследована специфика синдромов двойных ошибок в РС-кодах. Циклические и аффинные подстановки на РС-кодах порождают на них три вида групп автоморфизмов: Г, А и АГ. Соответственно определяются три вида орбит векторов-ошибок. Описана специфика спектров синдромов этих орбит ошибок. Показано, что эти спектры, как правило, являются полными. Структура спектров синдромов копирует структуру самих орбит, которые в свою очередь копируют структуру соответствующих групп автоморфизмов кода. Полученные результаты являются существенным вкладом в построение ТНС для кодов Рида-Соломона.

ЛИТЕРАТУРА

1. **McWilliams F. J., Sloan J. J.** The Theory of Error-Correcting Codes. – Amsterdam: North-holland publishing company; 1977. – 762 s.
2. **Скляр Б.** Цифровая связь. Теоретические основы и практическое применение. Изд. 2. – Москва: Вильямс; 2003–1104 с.
3. **Кудряшов Б. Д.** Основы теории кодирования. – Санкт-Петербург: БХВ-Петербург; 2016 – 400 с.
4. **Маров А. В., Утешев А. Ю.** Матричный формализм кодов Рида-Соломона // Вестник Санкт-Петербургского университета, Сер 10. Вып. 4. – Санкт-Петербург: БХВ-Петербург; 2016 – С. 4–17.

5. **Липницкий В. А. Конопелько В. К.** Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. – Минск: БГУ; 2007. – 239 с.

6. **Липницкий В. А., Семёнов С. И.** Автоморфизмы и орбиты ошибок кодов Рида-Соломона // Доклады БГУИР. Вып. 6 – Минск: БГУИР, 2019.

REFERENCES

1. **McWilliams F. J., Sloan J. J.** The Theory of Error-Correcting Codes. – Amsterdam: north-holland publishing company, 1977. – 762 s.

2. **Sclyar B.** Digital communications. Fundamentals and Applications. Ed. 2. – Moscow: Wil'ams; 2003–1104 s.

3. **Kudryashov B. D.** Fundamentals of coding theory. – St. Petersburg: BHV-Petersburg; 2016–400 s.

4. **Marov A. V., Uteshev A. Y.** Matrix formalism of Peed-Solomon codes // Vesnik Sanct-Peterburgskogo universiteta, Ser.10, V.4. – St. Petersburg: BHV-Petersburg; 2016 – s. 4–17.

5. **Lipnitsky V. A. Konopelko V. K.** Norm decoding of noise-resistant codes and algebraic equations. – Minsk: BGU; 2007–239 s.

6. **Lipnitsky V. A., Semyonov S. I.** The automorphisms and error orbits of Reed-Solomon codes // Doklady BGUIR V. 6 – Minsk: BGUIR, 2019. (In Russ.)

Поступила *20.01.2020* | *После доработки* *25.02.2020* | *Принята к печати* *01.03.2020*

LIPNITSKI V. A., SEMYONOV S. I.

SYNDROME SPECTRUMS OF ERROR ORBITS IN RS-CODES

Military academy Republic of Belarus

This article is devoted to the research of the properties of syndromes of errors in Reed-Solomon codes. RS-codes are built on non-binary alphabets. So, unlike BCH-codes, RS-codes contain an extremely large variety of correctable errors. To correct these errors, a systematic application of automorphisms of codes is proposed. Characteristic automorphisms of RS-codes are cyclic and affine substitutions forming cyclic groups Γ and A whose orders coincide with the code length. Cyclic and affine substitutions commute with each other and generate a joint AΓ group, what is the product of subgroups A and Γ. These three groups act on the space of error vectors of RS-codes, breaking this space into three types of error orbits. As a rule, these orbits are complete and contain the maximum possible number of errors. Syndromes are the main indicator of the presence of errors in each message received by the information system, a means of accurately identifying these errors. The specificity of syndromes of double errors in RS-codes is investigated. Determined that syndrome spectrums of error orbits are also complete in most cases. Proved that the structure of the syndrome spectrums copies the structure of the orbits themselves, which in turn copy the structure of groups of code automorphisms. The results obtained are a significant contribution to the construction of the theory of syndrome norms for RS-codes.

Keywords: *linear code, RS-code, error syndromes, automorphisms of codes, cyclic substitution, affine substitution, orbits of error vectors.*

Липницкий Валерий Антонович, профессор, доктор технических наук.
Lipnitski V. A., Doctor of technical sciences, professor.
E-mail: valipnitski@yandex.by.

Семёнов Сергей Иванович, адъюнкт кафедры информационно-вычислительных систем Военной академии Республики Беларусь
Semyonov S. I., the adjunct of chair of information and computing systems of Military academy Republic of Belarus.
E-mail: semyonov4213@gmail.com.