

## **ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И ПОМЕХОУСТОЙЧИВОСТИ КАНАЛОВ УПРАВЛЕНИЯ ТАКТИЧЕСКОГО ЗВЕНА РВ СВ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КОДОВ**

А.А. Кузнецов<sup>1</sup>, С.П. Евсеев<sup>1</sup>, С.В. Родионов<sup>1</sup>, А.А. Остренко<sup>2</sup>  
(<sup>1</sup>Харьковский университет Воздушных Сил, <sup>2</sup>в/ч А0162)

*Предлагается эффективный способ обеспечения безопасности и помехоустойчивости каналов управления тактического звена РВ СВ на основе использования симметричных криптосистем на эллиптических кодах.*

**помехоустойчивость, канал, тактическое звено, эллиптический код**

**Постановка проблемы.** Проведенный анализ показал, что в тактическом звене управления РВ СВ безопасность и помехоустойчивость каналов управления не отвечает современным требованиям. Важной военной научно-технической задачей является обеспечение требуемой безопасности и помехоустойчивости.

**Анализ литературы.** Перспективным направлением в решении поставленной задачи является разработка и исследование криптосистем, построенных на помехоустойчивых кодах [1 – 4]. В работах [1, 2] показано, что криптосистемы на обобщенных кодах Рида-Соломона могут быть взломаны алгоритмом с полиномиальной функцией сложности, а применение алгеброгеометрических кодов позволяет получить потенциально стойкую криптосистему. В работе [4] предложен эффективный метод несимметричного шифрования информации в АСУВ на основе алгеброгеометрических кодов, построенных по эллиптическим кривым (эллиптическим кодам).

**Цель статьи.** Исследование и разработка симметричных систем шифрования на эллиптических кодах, обоснование практических рекомендаций по их использованию для обеспечения безопасности и помехоустойчивости каналов управления тактического звена РВ СВ.

**Результаты исследований.** Для обеспечения автоматизированного протограммного обмена сообщениями в сетях и направлениях связи тактического звена АСУ РВ СВ применяется аппаратура передачи данных АПД 2506-Б1 (Т-244) «Базальт» [5]. Сообщения циркулируют по каналам связи между КШМ в виде протограмм, форма которых определяется используемой аппаратурой. Стандартная длина информационной части формализованных протограмм вместе с группой знаков ДСД (дополнение до стандартной длины) составляет 16, 58, 116, 206 и 396 знаков. Для повышения достоверно-

сти принимаемой информации при случайных и преднамеренных помехах используется группа знаков ГЗ (группа защиты), которая представляет собой 30-разрядную проверочную последовательность, вырабатываемую засекречивающей аппаратурой. Длина всего сообщения может составлять от 500 до 1500 знаков. Согласно тактико-техническим характеристикам [5] аппаратура Т-244 “Базальт” обеспечивает передачу формализованных кодограмм с показателем потери достоверности  $P_{\text{ош}} = 10^{-6}$ , что не соответствует современным требованиям к техническим средствам полевой сети передачи данных ( $P_{\text{тр}} = 10^{-9}$ ). Шифрование сообщений в аппаратуре Т-244 “Базальт” не предусмотрено. Таким образом, в существующей АСУ РВ используется аппаратура передачи данных и методы защиты информации, которые не удовлетворяют современным требованиям по достоверности (помехоустойчивости) и безопасности [6].

Перспективным направлением в развитии криптографических методов обработки информации является разработка теоретико-кодовых схем с использованием алгебраических кодов [1 – 4]. Основная идея, заложенная в эту конструкцию, состоит в использовании алгебраического блочного  $(n, k, d)$  кода, замаскированного под случайный код (код общего положения). Стойкость криптосистемы базируется на использовании теоретико-сложностной проблемы декодирования случайного кода.

Для построения симметричной криптосистемы на эллиптических кодах воспользуемся следующим определением [4].

*Определение.* Эллиптический  $(n, k, d)$  код над  $GF(q)$  это такой алгебро-геометрический код, который построен через отображение  $\varphi: EC \rightarrow P^{k-1}$  эллиптической кривой  $EC$ , его параметры связаны выражением  $k + d \geq n$ , причем:  $n \leq 2\sqrt{q} + q + 1$ ,  $k \geq \alpha$ ,  $d \geq n - \alpha$ , где  $\alpha$  – степень отображения  $\varphi$ .

Параметры симметричной теоретико-кодовой схемы на эллиптических кодах, определяются следующим утверждением.

*Утверждение.* Эллиптический  $(n, k, d)$  код над  $GF(q)$ ,  $q = 2^m$  определяет симметричную теоретико-кодовую схему с параметрами: размерность информационного вектора (в битах)  $l_1 = k \cdot m$ ; размерность криптограммы (в битах)  $l_2 = (2\sqrt{q} + q + 1) \cdot m$ ; относительная скорость передачи  $R = k / (2\sqrt{q} + q + 1)$ .

Для взлома криптосистемы, построенной на помехоустойчивом коде, необходимо решить задачу декодирования случайного кода. Наиболее эффективным способом является перестановочное декодирование.

Его сложность определяется выражением

$$I_{K+} = N_{\text{покр}} \cdot n \cdot (n - k),$$

где  $N_{\text{покр}} \geq C_n^t / C_{n-k}^t = (n(n-1) \dots (n-t-1)) / ((n-k)(n-k-1) \dots (n-k-t-1))$ .

На рис. 1 представлены зависимости  $I_{K^+}(m)$  в  $GF(2^m)$  для различных  $R = k/n$ . На рис. 2 представлены зависимости  $I_{K^+}(R)$  в  $GF(2^m)$ ,  $m = 5, \dots, 11$ . Проведенные исследования показывают, что потенциальной стойкими могут считаться криптосистемы, которые используют эллиптические коды, над  $GF(2^m)$ , где  $m \geq 8$ . При этом скорость кодирования должна стремиться к значению  $R = 1/2$ .

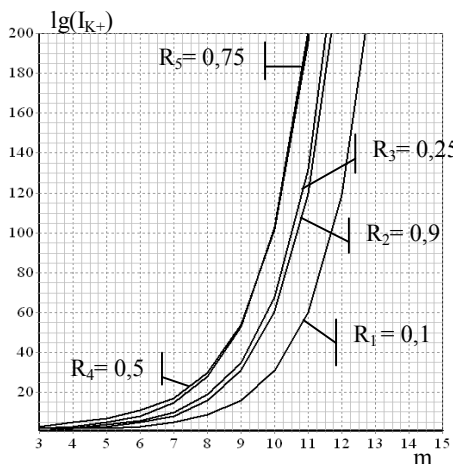


Рис. 1. Зависимость сложности взлома над  $GF(2^m)$  ( $R = \text{const}$ )

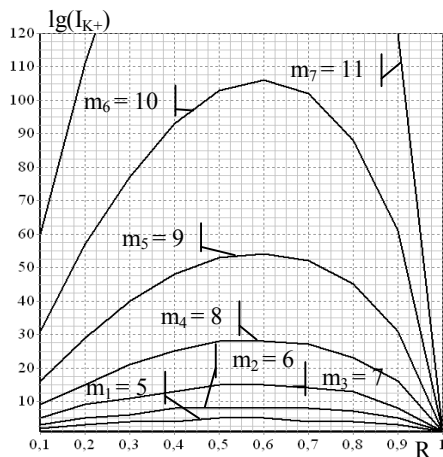


Рис. 2. Зависимость сложности взлома над  $GF(2^m)$  ( $m = \text{const}$ )

В табл. 1. приведены рекомендуемые кодовые параметры эллиптических кодов (EC) с  $R = 1/2$  для обеспечения безопасности и помехоустойчивости информации в тактическом звене АСУ РВ. Для сравнения в табл. 1 приведены так же параметры кодов Рида-Соломона (РС).

Таблица 1  
Кодовые характеристики EC и РС кодов над  $GF(2^8)$  и  $GF(2^9)$

GF(q)	EC			RS		
	n	k	d	n	k	d
$GF(2^8)$	289	144	145	255	127	129
$GF(2^9)$	557	276	281	511	255	257

Проведем исследования помехоустойчивости и криптостойкости, которую могут обеспечить симметричные теоретико-кодовые схема на эллиптических кодах. Зафиксируем  $(n, k, d)$  эллиптический код над  $GF(q)$ . Пусть  $e$  – вектор ошибок, который добавляется к кодовому слову при формировании криптограммы. Пусть  $w(e) \leq t$ ,  $t = \lfloor (d-1)/2 \rfloor$ . Обозначим долю веса вектора  $e$ , приходящегося на обеспечение безопасности, символом  $\rho = w(e) / t$ . Тогда потенциальная стойкость криптосистемы, по-

строенная на симметричной теоретико-кодовой схеме с эллиптическими кодами, будет определяться величиной  $\rho \cdot t$ , а помехоустойчивость передаваемых кодограмм определяться величиной  $(1 - \rho) \cdot t$ . На рис. 3 приведены зависимости криптостойкости  $I_{K+}(\rho)$  для рекомендуемых теоретико-кодовых схем на эллиптических кодах над  $GF(2^8)$  с  $R = 1/2$ . На рис. 4 приведены зависимости вероятности ошибки декодирования  $P_{\text{ош}}(\rho)$ . На рисунках приведены также зависимости криптостойкости и вероятности ошибки декодирования, соответствующие использованию РС кодов.

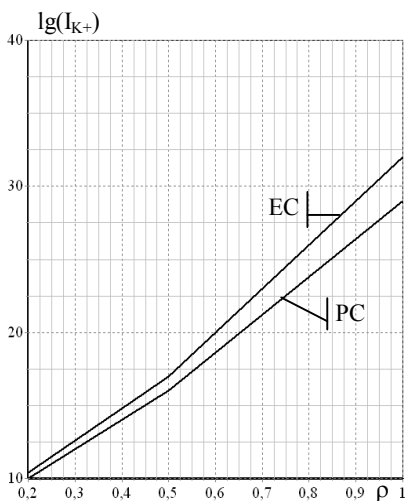


Рис. 3. Зависимости криптостойкости теоретико-кодовых схем на эллиптических кодах в  $GF(2^8)$

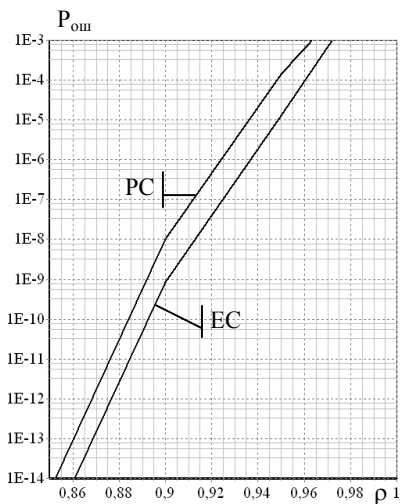


Рис. 4. Зависимости вероятности ошибки декодирования в теоретико-кодовых схемах на эллиптических кодах в  $GF(2^8)$

На рис. 5 приведены зависимости криптостойкости  $I_{K+}(\rho)$  для рекомендуемых теоретико-кодовых схем на эллиптических кодах над  $GF(2^9)$  с  $R = 1/2$ . На рис. 6 приведены зависимости вероятности ошибки декодирования  $P_{\text{ош}}(\rho)$ . На рисунках приведены также зависимости криптостойкости и вероятности ошибки декодирования, соответствующие использованию РС кодов. Очевидно, что коды ЕС по криптостойкости и помехоустойчивости превосходят коды РС. Рекомендуемое значение параметра  $\rho$  для обеспечения безопасности и помехоустойчивости каналов управления в АСУ РВ СВ составляет  $\rho = 0,8$ . Действительно, как видно из зависимостей приведенных на рис. 3 – 6, при  $\rho = 0,8$  криптосистемы на эллиптических кодах позволяют обеспечить высокие показатели безопасности и помехоустойчивости информации в АСУВ и решить поставленную военную научно-техническую задачу.

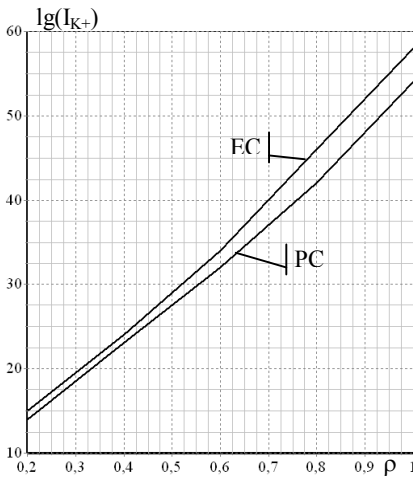


Рис. 5. Зависимости криптостойкости теоретико-кодowych схем на эллиптических кодах в  $GF(2^9)$

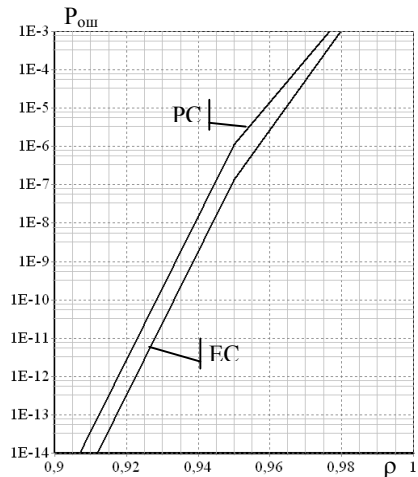


Рис. 6. Зависимости вероятности ошибки декодирования в теоретико-кодowych схемах на эллиптических кодах в  $GF(2^9)$

**Выводы.** Применение эллиптических кодов для криптографической защиты позволяет обеспечить требуемую безопасность и помехоустойчивость информации в АСУВ. Проведенные исследования особенностей обмена сообщениями в сетях и направлениях связи АСУ РВ СВ позволили обосновать практические рекомендации по использованию эллиптических кодов в криптографических целях, их криптостойкость и помехоустойчивость превышает аналогичные показатели для кодов Рида-Соломона.

## ЛИТЕРАТУРА

1. Сидельников В.М., Шестаков С.О. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона // *Дискретная математика*. – 1992. – Т. 4, № 3. – С. 57 – 63.
2. Сидельников В.М. Криптография и теория кодирования // *Материалы конференции «Московский университет и развитие криптографии в России»*. – М.: МГУ. – 2002. – 22 с.
3. Халимов Г.З., Северинов А.В. Обеспечение безопасности каналов передачи данных на основе помехоустойчивых кодов // *Системы управления и связь*. – Х.: ХВУ. – 1996. – С. 116 – 119.

Поступила 31.05.2005

**Рецензент:** доктор технических наук профессор Ю.В. Стасев,  
Харьковский университет Воздушных Сил.