УДК 681.325.3

ДИНАМИЧЕСКИЕ МОДЕЛИ КРИПТОСИСТЕМ С ЗАКРЫТЫМ КЛЮЧОМ. СИНТЕЗ ДЕШИФРАТОРОВ

А.А.Горбунов, К.Г.Кирьянов

Исследуется возможность построения за счет выбора алгебраической структуры дискретных динамических моделей криптосистем с закрытым ключом. Работа шифратора и дешифратора криптосистемы моделируется при помощи линейных цифровых автоматов. Рассмотрены временной (язык ABCD-формализма) и частотный (в виде *z*-преобразования) варианты данного подхода. Найдены условия возможности восстановления исходного сообщения по шифротексту применительно к обоим вариантам. Данные условия позволяют по имеющейся модели шифратора синтезировать модель дешифратора и, таким образом, синтезировать всю криптосистему в целом. Эффективность применения подобного подхода подтверждается на примерах конкретных криптосистем.

1. ВВЕДЕНИЕ

Одним из первых ввел и систематически исследовал простую и естественную *математическую модель* (ММ) шифра К. Шеннон в 1963 году в своей книге «Работы по теории информации и кибернетике» (раздел «Теория связи в секретных системах»). Он рассматривал так называемые “секретные системы”, в которых смысл сообщения скрывается при помощи шифра или кода, но само шифрованное сообщение не скрывается и предполагается, что противник обладает любым специальным оборудованием для перехвата и записи передаваемых сигналов [1, 2]. Считается, что текст сообщения должен быть зашифрован и состоит из последовательности дискретных по времени и значению символов, каждый из которых выбран из некоторого конечного множества символов - алфавита. Физически эти символы могут быть буквами или словами

некоторого языка, амплитудными уровнями квантованной речи или видеосигналом и т.д.

Нами для описания функционирования дискретных устройств, реализующих отдельные блоки шифратора и дешифратора криптосистемы (КС), применена теория *линейных цифровых автоматов* (ЛЦА), моделирующих работу многих дискретных устройств. Теория ЛЦА для нас удобна не только из-за её сравнительной простоты, но и из-за принципиальной возможности приведения нелинейных автоматов произвольного вида за счет выбора соответствующей алгебраической структуры (АС) ММ к форме ЛЦА [3]. ЛЦА является системой с конечным числом входных полюсов, к которым подводятся внешние сигналы, и с конечным числом выходных полюсов, на которых наблюдаются сигналы реакции. Основными свойствами такой системы являются дискретность компонент состояний (конечное поле возможных компонент состояний GF(q)) и дискретность времени (интервалы времени Δt между итерациями автомата – *такты*, величина которых принимается обычно за единицу измерения времени). Возможными способами математического представления модели ЛЦА являются “временной” (ABCD-формализм) и “частотный” (дискретное z-преобразование Цыпкина – Джури в полях Галуа или соответствующих кольцах) языки, описывающие эту модель в матричном виде. Относительно канала передачи шифротекста от шифратора к дешифратору предполагается, что он обладает малой временной задержкой по сравнению тактами автоматов ($\tau_K << \Delta t=1$).

В данной проблематике имеются вопросы, требующие дальнейшей проработки. Так, может оказаться достаточно полезным получать унифицированный вид ММ различных КС, иметь единые правила описания и синтеза различных элементов внутри самой КС. Например, представляет интерес:

синтез ММ дешифратора КС по имеющейся модели шифратора и наоборот; перенос результатов, полученных для одноканальных КС, на многоканальные (“многолучевые”), и т.д.

2. МОДЕЛИ КРИПТОСИСТЕМ С ЗАКРЫТЫМ КЛЮЧОМ НА ОСНОВЕ «ВРЕМЕННОГО» И «ЧАСТОТНОГО» ПОДХОДОВ

2.1. Шифратор как линейный цифровой автомат

Система уравнений, описывающая модель линейного цифрового автомата на языке ABCD-формализма, работающего в дискретном времени $t \in [0,1,2,\ldots,\infty]$, записывается следующим образом:

$$\begin{cases} x(t+1) = Ax(t) + Bu(t) \\ y(t) = Cx(t) + Du(t) \\ x(0) = x_0 \end{cases} \qquad (2.1)$$

В случае модели шифратора криптосистемы (КС) под входным сигналом ***u(t)*** подразумевается открытый текст, а под выходным сигналом ***y(t)*** – шифрограмма.

2.2. Дешифратор как линейный цифровой автомат

Основная идея восстановления входных сигналов по сигналам на выходе линейного цифрового автомата заключена в следующих выражениях:

$$\begin{cases} x(t+1) = Ax(t) + Bu(t) \\ Du(t) = y(t) - Cx(t) \\ x(0) = x_0 \end{cases} \qquad (2.2)$$

Если $\exists\, D^{-1}$:

$$\begin{cases} x(t+1) = Ax(t) + Bu(t) \\ u(t) = -D^{-1}Cx(t) + D^{-1}y(t) \\ x(0) = x_0 \end{cases} \qquad (2.3)$$

Подставляя в первое уравнение (2.3) вместо ***u(t)*** его значение, задаваемое вторым из уравнений (2.3) , имеем:

$$\begin{cases} x(t+1) = [A - BD^{-1}C]x(t) + [BD^{-1}]y(t) \\ u(t) = [-D^{-1}C]x(t) + [D^{-1}]y(t) \\ x(0) = x_0 \end{cases} \quad (2.4)$$

Таким образом, видим, что можно построить *восстанавливающий автомат* (*):

$$\begin{cases} x^*(t+1) = A^* x^*(t) + B^* u^*(t) \\ y^*(t) = C^* x^*(t) + D^* u^*(t) \\ x^*(0) = x_0{}^* = x_0 \end{cases} \quad (2.5)$$

т.к., если на вход автомата (2.5) поступает сигнал $\boldsymbol{u^*(t)=y(t)}$, то восстановленный сигнал $\boldsymbol{y^*(t)=u(t)}$ получим при условии

$$\exists\ D^{-1} \text{ и } A^*=[A-BD^{-1}C],\ B^*=[BD^{-1}],\ C^*=[-D^{-1}C],\ D^*=[D^{-1}],\ x_0{}^*=x_0\ . \quad (2.6)$$

Автомат (2.1) осуществляет преобразование входного сигнала ***u(t)*** в шифрсигнал ***y(t),*** а автомат (2.5) производит обратную операцию – преобразование зашифрованного сигнала $\boldsymbol{y(t)=u^*(t)}$ в исходный. Видим, что в качестве закрытого ключа КС в принципе могут быть использованы любые элементы в пяти матричных параметрах A, B, C, D и x_0.

2.3. «Частотный» подход к описанию ММ КС на основе коэффициентов передачи K(z)

В ряде технических приложений, иногда более удобной является схема описания ММ КС, опирающаяся на z-преобразование Цыпкина – Джури [4]:

$$Z[u(t)] \triangleq U(z) = \sum_{t=0}^{\infty} u(t)\, z^{-t} \bmod q \quad (2.7)$$

Преобразование (2.7) над системой уравнений ЛЦА (2.1) имеет следующий вид:

$$\begin{aligned} &u(t) \Rightarrow U(z),\quad y(t) \Rightarrow Y(z),\quad x(t) \Rightarrow X(z),\quad x(t+1) \Rightarrow z \cdot (X(z) - x_0) \\ &zX(z) - zx_0 = AX(z) + BU(z),\quad Y(z) = CX(z) + DU(z) \end{aligned} \quad (2.8)$$

Отсюда образ выходного сигнала $Y(z)$ выражается в следующем виде:

$$Y(z) = [C(zE - A)^{-1}B + D] \cdot U(z) + [zC(zE - A)^{-1}] \cdot x_0 \equiv K_1(z) \cdot U(z) + K_2(z) \cdot x_0\ , \quad (2.9)$$

где:
$$K_1(z) \equiv C(zE - A)^{-1}B + D \quad - \quad (2.10)$$
$$K_2(z) \equiv zC(zE - A)^{-1}$$

коэффициенты передачи шифрующего автомата.

К аналогичному виду приводятся и уравнения для дешифратора:

$$u^*(t) \Rightarrow U^*(z), \quad y^*(t) \Rightarrow Y^*(z), \quad x^*(t) \Rightarrow X^*(z), \quad x^*(t+1) \Rightarrow z \cdot (X^*(z) - x_0^*), \quad (2.11)$$
$$zX^*(z) - zx_0^* = A^*X^*(z) + B^*U^*(z), \quad Y^*(z) = C^*X^*(z) + D^*U^*(z)$$

$$Y^*(z) = [C^*(zE - A^*)^{-1}B^* + D^*] \cdot U^*(z) + [zC^*(zE - A^*)^{-1}] \cdot x_0^* \quad (2.12)$$

И введя *коэффициенты передачи дешифратора* следующим образом:

$$K_1^*(z) \equiv C^*(zE - A^*)^{-1}B^* + D^*, \quad (2.13)$$
$$K_2^*(z) \equiv zC^*(zE - A^*)^{-1}$$

получаем:

$$Y^*(z) = K_1^*(z) \cdot U^*(z) + K_2^*(z) \cdot x_0^* \quad (2.14)$$

Для канала связи имеем следующие уравнения:

$$u^*(t) = y(t) \quad \Rightarrow \quad U^*(z) = Y(z) \quad (2.15)$$

Таким образом:

$$Y^*(z) = K_1^*(z) \cdot U^*(z) + K_2^*(z) \cdot x_0^* = K_1^*(z) \cdot Y(z) + K_2^*(z) \cdot x_0^* =$$
$$= (K_1^*(z)K_1(z)) \cdot U(z) + K_1^*(z)K_2(z) \cdot x_0 + K_2^*(z) \cdot x_0^* \quad (2.16)$$

При точном восстановлении исходного текста из шифрованного в КС имеем равенство

$$Y^*(z) = U(z), \quad (2.17)$$

из которого получаем общий вид условия восстановления в частотной области:

$$(1 - K_1^*(z)K_1(z)) \cdot U(z) \quad = \quad K_1^*(z)K_2(z) \cdot x_0 + K_2^*(z) \cdot x_0^* \quad (2.18)$$

Полагая, что данное условие должно выполняться при произвольном входном сигнале *U(z)*, (2.18) можно переписать так:

$$\begin{cases} K_1^*(z) = (K_1(z))^{-1} \\ K_2^*(z) \cdot x_0^* = -K_1^*(z)K_2(z) \cdot x_0 \end{cases} \quad (2.19)$$

Рассматривая частный случай равенства начальных состояний шифрующего и дешифрующего автоматов, приходим к условию восстановления, записанному через коэффициенты передачи, которое выглядит следующим образом:

$$\begin{cases} K_1^*(z) = (K_1(z))^{-1} \\ K_2^*(z) = -(K_1(z))^{-1} \cdot K_2(z) \\ x_0^* = x_0 \end{cases} \quad (2.20)$$

или:

$$\begin{cases} C^* \cdot (zE - A^*)^{-1} \cdot B^* + D^* = (C \cdot (zE - A)^{-1} \cdot B + D)^{-1} \\ zC^* \cdot (zE - A^*)^{-1} = -(C \cdot (zE - A)^{-1} \cdot B + D)^{-1} \cdot zC \cdot (zE - A)^{-1} \end{cases} \quad (2.21)$$

Путем несложных преобразований над правыми частями уравнений систему (2.21) можно привести к виду:

$$\begin{cases} C^* \cdot (zE - A^*)^{-1} \cdot B^* + D^* = -D^{-1}C \cdot (zE - (A - BD^{-1}C))^{-1} \cdot BD^{-1} + D^{-1} \\ zC^* \cdot (zE - A^*)^{-1} = -z \cdot D^{-1}C \cdot (zE - (A - BD^{-1}C))^{-1} \end{cases}, \quad (2.22)$$

Из (2.22) видно, что при выполнении соотношений (2.6) между матрицами шифрующего и дешифрующего автоматов, выполняются и условия восстановления (2.18-2.20), выраженные через коэффициенты передачи.

3. ПРИМЕНЕНИЕ ПОДХОДОВ К ОПИСАНИЮ КОНКРЕТНЫХ СИСТЕМ ШИФРОВАНИЯ

В данном разделе на конкретных примерах классических методов шифрования (система шифрования Цезаря, система шифрования Вижинера, шифрование методом гаммирования) показаны способы приведения описания КС к рассмотренному выше представлению в виде линейных динамических систем. Для КС необходимо учитывать в какой АС будет строиться модель. В некоторых случаях удается обойтись алгебраической структурой GF(q) – полем Галуа или соответствующим кольцом GK(q) (дискретных элементов) по модулю q, когда под

операциями сложения “+” и вычитания “-” в формулах и подразумеваются операции по модулю q. В первых трех из рассматриваемых ниже примеров, модели шифратора и дешифратора строятся в алгебраической структуре GK(q). Значение q равняется размерности алфавита и, например, для английского алфавита q=26.

Однако так сделать получается далеко не всегда. В более сложных примерах для сведения ММ к уровню ABCD-формализма приходится в качестве сложения и вычитания вводить особые операции, что приводит уже к совершенно иным АС, нежели GF(q) или GK(q). Таким примером может служить шифр обычной замены в соответствие с заранее заданной таблицей, рассматриваемой в качестве ключа (например, шифр Петра I). В данном случае построение ММ криптосистемы на языке ABCD-формализма требует рассмотрения операции “сложения числа с вектором”.

3.1. Система шифрования Цезаря

При шифровании по данному методу каждая буква исходного текста заменяется другой буквой того же алфавита по следующему правилу. Замещающая буква определялась путем смещения по алфавиту от исходного символа на К позиций. При достижении конца алфавита выполнялся циклический переход к его началу [2, с.47]. Цезарь использовал шифр замены при смещении К=3. При описании на уровне динамической системы алгоритм шифрования может быть описан следующим выражением:

$$y = (u + K) \bmod q \ . \qquad (3.1)$$

Схема цифрового автомата, выполняющего шифрование Цезаря, представлена на рис 3.1.

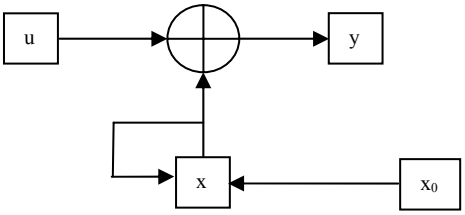

Рис. 3.1. Схема шифрования Цезаря

На языке ABCD-формализма систему можно представить следующим образом:

$$\begin{cases} x(t+1) = x(t) \\ y(t) = x(t) + u(t) \\ x(0) = x_0 = K \end{cases} \tag{3.2}$$

Т. е. $A = [1]$, $B = [0]$, $C = [1]$, $D = [1]$, $x_0 = K$.

Для восстанавливающего автомата (ABCD-модель дешифратора) по формулам (2.4)-(2.6) имеем:

$$A^*=A-BD^{-1}C=A=[1]\ ,\quad B^*=[BD^{-1}]=[0]\ ,\quad C^*=[-D^{-1}C]=[-1]\ ,\quad D^*=[D^{-1}]=[1]\ ,$$

$$x_0{}^*=x_0=K\ . \tag{3.3}$$

$$\begin{cases} x^*(t+1) = x^*(t) \\ y^*(t) = -x^*(t) + u^*(t) \\ x^*(0) = x_0{}^* = x_0 = K \end{cases} \quad \text{или} \quad \begin{cases} x(t+1) = x(t) \\ u(t) = y(t) - x(t) \\ x(0) = x_0 = K \end{cases} \tag{3.4}$$

3.2. Система шифрования Вижинера

Система Вижинера подобна такой системе шифрования Цезаря, у которой ключ подстановки меняется от буквы к букве [2, с.62]. Последовательность ключей обычно получают из числовых значений букв ключевого слова. Если ключ оказался короче сообщения, то его циклически повторяют. Схема цифрового автомата, выполняющего шифрование по Вижинеру и обладающего памятью для хранения ключевого слова длиной в три символа, представлена на рис. 3.2.

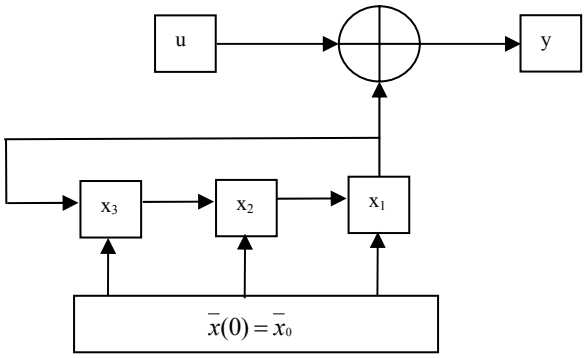

Рис. 3.2. Схема шифрования Вижинера

Линейный цифровой автомат, осуществляющий шифрование Вижинера, на языке ABCD-формализма описывается следующим образом:

$$\begin{cases} x_1(t+1) = x_2(t) \\ x_2(t+1) = x_3(t) \\ x_3(t+1) = x_1(t) \\ y(t) = x_1(t) + u(t) \\ \bar{x}(0) = \bar{x}_0 = \begin{bmatrix} x_{1\_0} \\ x_{2\_0} \\ x_{3\_0} \end{bmatrix} \end{cases} \tag{3.5}$$

т.е. матрицы имеют вид:

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad C = [\,1 \quad 0 \quad 0\,] \quad D = [\,1\,] \quad \bar{x}_0 = \begin{bmatrix} x_{1\_0} \\ x_{2\_0} \\ x_{3\_0} \end{bmatrix} \tag{3.6}$$

Тогда матрицы восстанавливающего автомата, получающиеся из исходных по формулам (2.6), примут вид:

$$A^* = A\text{-}BD^{-1}C = A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \qquad B^* = BD^{-1} = B = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$C^* = -D^{-1}C = [\,-1 \quad 0 \quad 0\,] \qquad D^* = D^{-1} = [\,1\,] \qquad \bar{x}_0^* = \bar{x}_0 = \begin{bmatrix} x_{1\_0} \\ x_{2\_0} \\ x_{3\_0} \end{bmatrix} \tag{3.7},$$

а система уравнений для модели дешифратора на языке ABCD-формализма запишется, в соответствие с (2.4)-(2.6), так:

$$\begin{cases} x^*_1(t+1) = x^*_2(t) \\ x^*_2(t+1) = x^*_3(t) \\ x^*_3(t+1) = x^*_3(t) \\ y^*(t) = -x^*_1(t) + u^*(t) \\ \bar{x}^*(0) = \bar{x}^*_0 = \bar{x}_0 = \begin{bmatrix} x_{1\_0} \\ x_{2\_0} \\ x_{3\_0} \end{bmatrix} \end{cases} \quad \text{или} \quad \begin{cases} x_1(t+1) = x_2(t) \\ x_2(t+1) = x_3(t) \\ x_3(t+1) = x_1(t) \\ u(t) = y(t) - x_1(t) \\ \bar{x}(0) = \bar{x}_0 = \begin{bmatrix} x_{1\_0} \\ x_{2\_0} \\ x_{3\_0} \end{bmatrix} \end{cases} \tag{3.8}$$

3.3. Система с гаммированием

Под гаммированием понимают процесс наложения по определенному закону гаммы шифра на открытые данные. Гамма шифра – это псевдослучайная последовательность, выработанная по заданному алгоритму для зашифровывания открытых данных и расшифрования зашифрованных данных [2, с.73]. На рис. 3.3 приведена схема одного из примеров линейного цифрового автомата, осуществляющего шифрование методом гаммирования.

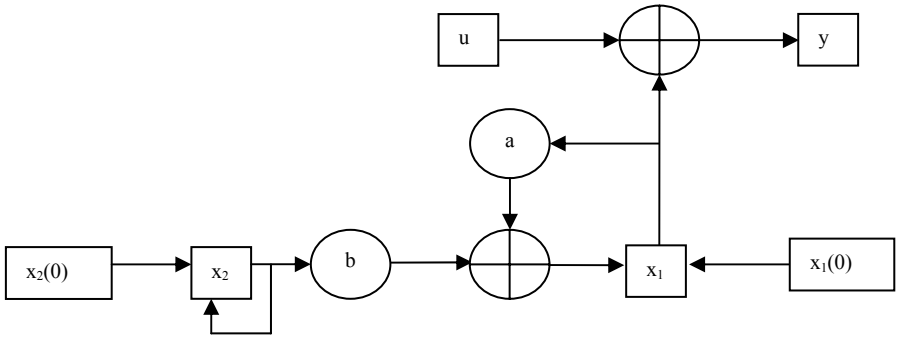

Рис. 3.3. Схема шифрования методом гаммирования

Псевдослучайная последовательность чисел здесь вырабатывается линейным конгруэнтным генератором, который описывается следующим соотношением:

$$x_1(n+1) = \{ax_1(n) + b\} \bmod q \ .$$

Соответственно система уравнений, описывающих данный шифратор, имеет вид:

$$\begin{cases} x_1(t+1) = ax_1(t) + bx_2(t) \\ x_2(t+1) = x_2(t) \\ y(t) = x_1(t) + u(t) \\ x(0) = x_0 = \begin{bmatrix} x_{1\ 0} \\ 1 \end{bmatrix} \end{cases} \tag{3.9}$$

т.к. ее матрицы представляются следующим образом:

$$A=\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \quad B=\begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad C=\begin{bmatrix} 1 & 0 \end{bmatrix} \quad D=\begin{bmatrix} 1 \end{bmatrix} \quad x_0=\begin{bmatrix} x_{1\,0} \\ 1 \end{bmatrix} \tag{3.10}$$

Применяя к данным матрицам выражения (2.6), получаем для дешифратора:

$$A^*=A=\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \quad B^*=\begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad C^*=-D^{-1}C=\begin{bmatrix} -1 & 0 \end{bmatrix} \quad D^*=D^{-1}=\begin{bmatrix} 1 \end{bmatrix} \quad x_0=x^*{}_0=\begin{bmatrix} x_{1\,0} \\ 1 \end{bmatrix} \tag{3.11}$$

и систему уравнений, описывающих дешифратор:

$$\begin{cases} x^*{}_1(t+1)=ax^*{}_1(t)+bx^*{}_2(t) \\ x^*{}_2(t+1)=x^*{}_2(t) \\ y^*(t)=-x^*{}_1(t)+u^*(t) \\ x^*(0)=x^*{}_0=x_0=\begin{bmatrix} x_{1\,0} \\ 1 \end{bmatrix} \end{cases} \quad \text{или:} \quad \begin{cases} x_1(t+1)=ax_1(t)+bx_2(t) \\ x_2(t+1)=x_2(t) \\ u(t)=y(t)-x_1(t) \\ x(0)=x_0=\begin{bmatrix} x_{1\,0} \\ 1 \end{bmatrix} \end{cases} \tag{3.12}$$

3.4. Система *с гаммированием. Подход на основе коэффициентов передачи*

Рассмотрим модель системы шифрования методом гаммирования в частотной области (на языке *z*-преобразования (2.7)). Выражения для коэффициентов передачи шифратора (2.10) в данном случае принимают вид:

$$\begin{aligned} &K_1(z)\equiv C(zE-A)^{-1}B+D=\begin{bmatrix} 1 \end{bmatrix} \\ &K_2(z)\equiv zC(zE-A)^{-1}=z\begin{bmatrix} 1 & 0 \end{bmatrix}\cdot\begin{bmatrix} z-a & -b \\ 0 & z-1 \end{bmatrix}^{-1}=\frac{z}{(z-a)\cdot(z-1)}\begin{bmatrix} (z-1) & b \end{bmatrix} \end{aligned} \tag{3.13}$$

Следовательно, выражение для изображения последовательности шифротекста Y(z) представляется как:

$$\begin{aligned} &Y(z)=K_1(z)\cdot U(z)+K_2(z)\cdot x_0=U(z)+\frac{z}{(z-a)\cdot(z-1)}\begin{bmatrix} (z-1) & b \end{bmatrix}\cdot\begin{bmatrix} x_{1\,0} \\ 1 \end{bmatrix}= \\ &=U(z)+\frac{z\cdot((z-1)\,x_{1\,0}+b)}{(z-a)\cdot(z-1)} \end{aligned} \tag{3.14}$$

Для коэффициентов передачи дешифратора в соответствие с (2.14) имеем:

$$\begin{aligned} &K_1^*(z)\equiv C^*(zE-A^*)^{-1}B^*+D^*=\begin{bmatrix} 1 \end{bmatrix} \\ &K_2^*(z)\equiv zC^*(zE-A^*)^{-1}=z\begin{bmatrix} -1 & 0 \end{bmatrix}\cdot\begin{bmatrix} z-a & -b \\ 0 & z-1 \end{bmatrix}^{-1}=\frac{-z}{(z-a)\cdot(z-1)}\begin{bmatrix} (z-1) & b \end{bmatrix} \end{aligned} \tag{3.15}$$

Как видно, условия восстановления в частотной области (2.20) выполняются. Выражение для образа самого восстановленного сигнала (см. (2.16)) запишется следующим образом:

$$Y^*(z) = K_1^*(z)\cdot U^*(z) + K_2^*(z)\cdot x_0^* = U^*(z) - \frac{z}{(z-a)\cdot(z-1)}\begin{bmatrix}(z-1) & b\end{bmatrix}\cdot\begin{bmatrix}x_{1\ 0}\\ 1\end{bmatrix} = \\ = U^*(z) - \frac{z\cdot((z-1)\,x_{1\ 0}+b)}{(z-a)\cdot(z-1)} \qquad (3.16)$$

3.5. Система шифрования Петра I. Пример формализации в нестандартной АС

Внешне шифр Петра I [5, с.52] представляет собой таблицу замены: под горизонтально расположенными в алфавитной последовательности буквами кириллицы или иной азбуки, соответствующей языку открытого сообщения, подписаны элементы соответствующего шифроалфавита. Для представления модели данной криптосистемы в ABCD-формализме приходится выходить за пределы алгебраической структуры GK(q) и вводить в качестве операции сложения *нелинейную* индексную операцию над вектором и числом – операцию *сложения по индексу*. Если вектор $\boldsymbol{z}$ содержит **n=q** различных целочисленных компонент из диапазона от **1** до **q**, а целое число $\boldsymbol{u}$ также принадлежит этому диапазону, то операция сложения по индексу между $\boldsymbol{z}$ и $\boldsymbol{u}$ вводится как:

$$\boldsymbol{z} \oplus_i \boldsymbol{u} = \begin{bmatrix} z_1 \\ z_2 \\ \dots \\ z_q \end{bmatrix} \oplus_i \boldsymbol{u} = \boldsymbol{z_u} = \begin{cases} z_1, & \text{если } u = 1 \\ z_2, & \text{если } u = 2 \\ \cdots & \\ z_q, & \text{если } u = q \end{cases} \qquad (3.17)$$

Операция, обратная к данной, вводится следующим образом:

$$\boldsymbol{z} \oplus_i^{-1} \boldsymbol{u} = \begin{bmatrix} z_1 \\ z_2 \\ \dots \\ z_q \end{bmatrix} \oplus_i^{-1} \boldsymbol{u} = \begin{cases} 1, & \text{если } u = z_1 \\ 2, & \text{если } u = z_2 \\ \cdots & \\ q, & \text{если } u = z_q \end{cases} \qquad (3.18)$$

и может быть названа *извлечением индекса*.

При построении модели данной КС под ключом будем понимать вектор ***z***, содержащий последовательность из ***q*** номеров символов шифроалфавита, причем порядок расположения этих символов соответствует таблице замены шифра. Тогда, имея ввиду применение операции сложения по индексу вектора и числа, будем считать внутреннее состояние системы вектором, которое определяется ключом ***z***. Подразумевая в дальнейшей записи под суммированием "+" сложение по индексу "$\oplus_i$", а под вычитанием "–" – обратную ей операцию извлечения индекса "$\oplus_i^{-1}$", имеем следующую систему уравнений, описывающих шифратор на языке ABCD-формализма:

$$\begin{cases} x(t+1) = x(t) \\ y(t) = x(t) + u(t) \\ x(0) = z \end{cases} \tag{3.19}$$

т. е. $A=E$, $B=0$, $C=E$, $D=1$, $x_0=\mathbf{z}$. (E – единичная матрица).

Для восстанавливающего автомата (ABCD-модель дешифратора) по формулам (2.4)-(2.6) имеем:

$$A^*=A-BD^{-1}C=A=E,\quad B^*=[BD^{-1}]=[0]\,,\quad C^*=[-D^{-1}C]=-E\,,\quad D^*=[D^{-1}]=[1]\,,\quad x_0^*=x_0=\mathbf{z}\,. \tag{3.20}$$

$$\begin{cases} x^*(t+1) = x^*(t) \\ y^*(t) = -x^*(t) + u^*(t) \\ x^*(0) = x_0^* = x_0 = z \end{cases} \quad \text{или} \quad \begin{cases} x(t+1) = x(t) \\ u(t) = y(t) - x(t) \\ x(0) = x_0 = z \end{cases} \tag{3.21}$$

4. РЕЗУЛЬТАТЫ ОБРАБОТКИ ТЕСТОВЫХ ПРИМЕРОВ

Описанный в работе подход был реализован практически в виде программ построения матриц дешифрующего ЛЦА по матрицам шифрующего (на основе формул (2.6), хотя, как следует из настоящей работы, возможен вариант ее реализации на основе формул (2.18)-(2.20)), а также программы, осуществляющей действия самого автомата. Данные программы позволяют переходить от ММ

конкретного линейного автомата (шифратора) к модели КС в целом и соответственно восстанавливать выходной сигнал шифратора.

В качестве тестовых примеров использовались модели автоматов, реализующих операции шифрования и дешифрования исходного текста, символы которого задаются своими номерами в алфавите. Рассмотрены следующие виды шифрования: шифр Цезаря (3.2), шифр Вижинера (3.5), шифрование методом гаммирования (3.9) на основе псевдослучайной последовательности, вырабатываемой линейным конгруэнтным генератором и шифр Петра I (3.19). Результаты обработки тестовых примеров представлены в табл. 4.1.

Табл. 4.1

Метод шифро-вания	Матрицы, параметры КС	Входная последовательность – исходный текст – ***u(t)***	Выходная последовательность – шифротекст – ***y(t)***	Восстановленная последовательность – $\boldsymbol{u}^*(t)$	q
Шифр Цезаря [2]	(3.2), (3.3) K=3	1 2 3 4 5 6 7 8 9 0	4 5 6 7 8 9 0 1 2 3	1 2 3 4 5 6 7 8 9 0	10
		3 0 9 4 2 5 9 1 2 0 4 3 8 6 1 7	6 3 2 7 5 8 2 4 5 3 7 6 1 9 4 0	3 0 9 4 2 5 9 1 2 0 4 3 8 6 1 7	10
Шифр Вижинера [2]	(3.6), (3.7) x_{1_0}=3, x_{2_0}=7, x_{3_0}=5	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	3 7 5 3 7 5 3 7 5 3 7 5 3 7 5 3	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	10
		0 1 2 3 4 5 6 7 8 9 8 7 6 5 4 3 2 1 0	3 8 7 6 1 0 9 4 3 2 5 2 9 2 9 6 9 6 3	0 1 2 3 4 5 6 7 8 9 8 7 6 5 4 3 2 1 0	10
Гаммиро-вание [2]	(3.10), (3.11), a=7, b=13 x_{1_0}=2, x_{2_0}=1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	3 5 19 2 21 16 4 12 22 0 7 10 8 17 11 15 20 9 1 14 13 6 3 5	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	23
		0 1 2 3 4 5 6 7 8 9 8 7 6 5 4 3 2 1 0	2 5 20 4 1 20 9 18 6 8 14 16 13 21 14 17 21 9 0	0 1 2 3 4 5 6 7 8 9 8 7 6 5 4 3 2 1 0	23
	(3.10), (3.11), a=777, b=901 x_{1_0}=23, x_{2_0}=47	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	23 58 117 136 51 54 81 68 207 178 173 128 235 174 137 60 135 42 229 120 163 38 193 52	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	256
		0 0 255 255 48 32 75 117 36 4 90 255 255 0 0 0 0 0	23 58 116 135 99 86 156 185 243 182 7 127 234 174 137 60 135 42	0 0 255 255 48 32 75 117 36 4 90 255 255 0 0 0 0 0	256
Шифр Петра I [5]	(3.19), (3.20), $x_0 = [5\ 2\ 1\ 3\ 8\ 7\ 6\ 4]^T$	3 4 2 7 5 5 8 1 3 4 6 1 7 1 3	1 3 2 6 8 8 4 5 1 3 7 5 6 5 1	3 4 2 7 5 5 8 1 3 4 6 1 7 1 3	–
		1 8 4 6 3 6 32 4 7 1 5 32 2 1	5 4 3 7 1 7 32 3 6 5 8 32 2 5	1 8 4 6 3 6 32 4 7 1 5 32 2 1	–

5. ЗАКЛЮЧЕНИЕ

1) Показано, что для математических моделей всех рассмотренных нами известных КС с закрытым ключом (шифратор, дешифратор) за счёт выбора соответствующей алгебраической структуры этих моделей:

– *возможно описание* (*представление*) на языке линейных динамических систем в полях Галуа как во временной (в форме ABCD-формализма), так и в частотной (на языке *z*-преобразования) областях;

– приведены соотношения (2.6), позволяющие *строить модель дешифратора по* имеющейся *модели шифратора*, расширяющие математическое описание модели на всю криптосистему в целом;

– сформулированы *условия возможности восстановления* исходного сообщения по шифротексту во временной (2.6) и в частотной (в виде связей между коэффициентами передачи *K(z)*, (2.18-2.20)) моделях шифратора и дешифратора;

– приведены примеры (система шифрования Цезаря, система шифрования Вижинера, шифрование методом гаммирования, нелинейный шифр Петра I) подтверждающие возможность рассмотрения теории КС в форме линейных дискретных динамических моделей.

2) Результаты могут представить интерес при преподавании курсов теории автоматического управления, теории колебаний, дискретной математики, основ криптографии и криптоанализа с *единых методических позиций автоматического управления*, так как в даже наиболее полных справочных изданиях по автоматическому управлению (см., напр. [6]) материал, относящийся к работе КС в полях Галуа, обычно не приводится.

3) Разнообразие рассмотренных примеров, в том числе и не описанных в настоящей работе, позволяет сделать предположение о том, что для значительного числа прочих криптосистем математические модели могут быть описаны на языке линейных и сводящихся к ним дискретных динамических систем.

Работа выполнена при частичной поддержке РФФИ (грант 02-02-17573).

ЛИТЕРАТУРА

1. Шеннон Клод. Теория связи в секретных системах. //В кн. Работы по теории информации и кибернетике. Пер. В.Ф. Писаренко. М.: ИЛ, 1963.- С. 333–369

2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.

3. Гилл А. Линейные последовательностные машины: Перев. с англ. М.: Наука, Гл. редакция физ.-мат. литературы, 1974.

4. Кирьянов К.Г. К теории сигнатурного анализа. //В ж. Техника средств связи. Вып. 2. М.: ЭКОС, 1980. С. 1–46.

5. Соболева Т.А. Тайнопись в истории России (история криптографической службы России XVIII – XX вв.). М.: Международные отношения, 1994.

6. Справочник по теории автоматического управления. /Под ред. А.А. Красовского. М.: Наука, Гл. редакция физ.-мат. литературы, 1987.