ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF EDUCATION AND SCIENCE
OF THE REPUBLIC OF KAZAKHSTAN

Л.Н. ГУМИЛЕВ АТЫНДАҒЫ
ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ
ЕВРАЗИЙСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ ИМ. Л.Н. ГУМИЛЕВА
GUMILYOV EURASIAN
NATIONAL UNIVERSITY

ЖАС ҒАЛЫМДАР КЕҢЕСІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2015» атты X Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ X Международной научной конференции студентов и молодых ученых «Наука и образование - 2015»

PROCEEDINGS of the X International Scientific Conference for students and young scholars «Science and education - 2015»

УДК 001:37.0
ББК72+74.04
Ғ 96

Ғ96
«Ғылым және білім – 2015» атты студенттер мен жас ғалымдардың X Халық. ғыл. конф. = X Межд. науч. конф. студентов и молодых ученых «Наука и образование - 2015» = The X International Scientific Conference for students and young scholars «Science and education - 2015». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie-2015/, 2015. – 7419 стр. қазақша, орысша, ағылшынша.

ISBN 978-9965-31-695-1

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001:37.0
ББК 72+74.04

ISBN 978-9965-31-695-1

УДК 004.056.55

РЕАЛИЗАЦИЯ ОДНОГО ПРИМЕРА КОНЕЧНО-АВТОМАТНОЙ КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧЕМ FAPKC

Сауханов Султангазы Нургазыевич
saukhanov@gmail.com

Магистрант 2-го курса, специальность «6М060200-Информатика»
ЕНУ им. Л.Н.Гумилева, Астана, Қазақстан
Научный руководитель – А.Шарипбай

Идея использоавния автоматной модели в криптографии с открытым ключом не является новой. В Китае с 80-х годов прошлого века ведутся работы в области создания асимметричных криптосистем, основанных на конечных автоматах [1].

В основе теории класса конечно-автоматных криптосистем с открытым ключом, известных по сокращённым названием FAPKC – FiniteAutomationPublicKeyCryptosystems, лежит понятие автомата, слабо обратимого с конечной задержкой τ. Так называется конечный автомат, в котором любое слово во входной последовательности однозначно определяется по соответствующему начальному состоянию слову выходной последовательности и по следующим за этим словом τ выходным символом.

Рассмотрим FAPKC в случае, когда шифрование состоит в преобразовании автоматомM_fв состоянии q открытого текста, дополненного суффиксом длиной τ, а расшифрование – в преобразовании шифртекста автоматом M' в соответствующем состоянии q'и удалении из результата преобразования префикса длиной τ[2].

Данный автомат FAPKCсводятся к вычислениям

$$\beta = \bar{\varphi}_f(\alpha\xi, q);\ \zeta\alpha = \bar{\varphi}'(\beta, q'), \tag{1}$$

где β выходное слово (шифртекст), которую вырабатывает автомат пробегая из состояния q под действием входного слова α дополненное ξ- суффиксом длиной τ, $\zeta\alpha$ выходное слово (исходный текст, дополненное ζ – префиксом длиной τ.), которую вырабатывает обратный автомат пробегая из состояния q' под действием β шифротектста.

Для любого автомата $M =< X, Q, Y, \psi, \varphi >$и любого целого $\tau \geq 0$ автомат $M^{(\tau)} =< X, Q \times \{0,1,\dots,\tau\}, Y, \psi^{(\tau)}, \varphi^{(\tau)} >$определяется как

$$\psi^{(\tau)}\big(x,(q,i)\big) = \begin{cases}(q, i+1), & 0 \leq i < \tau,\\ (\psi(x,q),\tau), & i = \tau,\end{cases} \tag{2}$$

$$\varphi^{(\tau)}\big(x,(q,i)\big) = \begin{cases}y_0, & 0 \leq i < \tau\\ \varphi(x,q), & i = \tau\end{cases} \tag{3}$$

В формулах (1)-(3) функции переходов и выходов однозначно определяется с помощью входо-выходной функции a автомата:

$$y_t = f(x_{t-h}x_{t-h+1}\dots x_t y_{t-k}y_{t-k+1}\dots x_{t-1}),\ t = 0,1,\dots \tag{4}$$

Рассмотрим пример FAPKC [3]. Даны автоматы f_2линейный с характеристиками $h_2=2$, $\tau_2=1$и входо-выходными уравнениями

$$z_t = y_{t-2} + y_{t-1},\ t \geq 0 \tag{5}$$

и автомат f_1нелинейный с характеристиками $h_1=2$, $\tau_1=0$ и входо-выходными уравнениями

$$y_t = x_t + x_{t-1} + x_{t-2}x_{t-1},\ t \geq 0 \tag{6}$$

Подставляя (2) в (1), получим входо-выходные уравнения для $f=f_1f_2$:

$$z_t = x_{t-1} + x_{t-3} + x_{t-4}x_{t-3} + x_{t-3}x_{t-2},\ t \geq 0 \tag{7}$$

Таким образом, $h = 4, \tau = 1; M_{fi} =< \{0,1\}, \{0,1\}^2, \{0,1\}, \psi_i, \varphi_i >, i = 1,2;\ M_f =< \{0,1\}, \{0,1\}^4, \{0,1\}, \psi_f, \varphi_f >$и функции переходов и выходов этих автоматов заданы следующими таблицами:

Таблица 1. Функция переходаψ_1

	$x_{-2}x_{-1}$			
x_0	00	01	10	11
0	00	10	00	10
1	01	11	01	11

Таблица 2. Функция выхода φ_1

	$x_{-2}x_{-1}$			
x_0	00	01	10	11
0	0	1	0	0
1	0	0	0	1

Таблица 3. Функция перехода ψ_2

	$y_{-2}y_{-1}$			
x_0	00	01	10	11
0	00	10	00	10
1	01	11	01	11

Таблица 4. Функция выхода φ_2

	$y_{-2}y_{-1}$			
y_0	00	01	10	11
0	0	1	1	0
1	0	1	1	0

Таблица переходов определяется следующей формулой*:* $\psi(x_0, x_{-h}, x_{-h+1} \dots x_{-1} y_{-k} y_{-k+1} \dots y_{-1} = (x_{-h+1} \dots x_{-h} x_0 y_{-k+1} \dots y_{-2} y_{-1})$.

Таблица выходов определяется следующей формулой*:* $f(x_{-h} \dots x_{-1} x_0 y_{-k} y_{-k+1} \dots y_{-1} = \varphi(x_0, x_{-h} x_{-h+1} \dots x_{-1} y_{-k} y_{-k+1} \dots y_{-1})$.

Таблица 5. Функция перехода ψ_f

	$x_{-4}x_{-3}x_{-2}x_{-1}$							
x_0	0000	0001	0010	0011	0100	0101	0110	0111
0	0000	0010	0100	0110	1000	1010	1100	1110
1	0001	0011	0101	0111	1001	1011	1101	1111

Таблица 6. Функция перехода ψ_fпродолжение

	$x_{-4}x_{-3}x_{-2}x_{-1}$							
x_0	1000	1001	1010	1011	1100	1101	1110	1111
0	0000	0010	0100	0110	1000	1010	1100	1110
1	0001	0011	0101	0111	1001	1011	1101	1111

Таблица 7. Функция выхода φ_f

	$x_{-4}x_{-3}x_{-2}x_{-1}$							
x_0	0000	0001	0010	0011	0100	0101	0110	0111
0	0	1	0	1	1	0	0	1
1	0	1	0	1	1	0	0	1

Таблица 8. Функция выхода φ_fпродолжение

	$x_{-4}x_{-3}x_{-2}x_{-1}$							
x_0	1000	1001	1010	1011	1100	1101	1110	1111
0	0	1	0	1	0	1	1	0
1	0	1	0	1	0	1	1	0

Функция φ_1в каждом состоянии, поэтому автомат f_1 действительно обратим с задержкой $\tau_1 = 0$. В обратном к нему с задержкой 0 автомате $M_1^{'} =< \{0,1\}, \{0,1\}^2, \{0,1\}, \psi_1^{'}, \varphi_1^{'} >$функции $\psi_1^{'}, \varphi_1^{'}$получаются по правилу: если $\psi_1(x,q) = s$и$\varphi_1(x,q) = y$, то $\psi_1^{'}(y,q) = s$и$\varphi_1^{'} = x$.Полученный так, они показаны в следующих таблицах:

Таблица 9. Функция перехода $\psi_1^{'}$

	$x_{-2}x_{-1}$			
x_0	00	01	10	11
0	00	11	00	10
1	01	10	01	11

Таблица 10. Функция выхода $\varphi_1^{'}$

	$x_{-2}x_{-1}$			
y_0	00	01	10	11
0	0	1	0	0
1	1	0	1	1

Входо-выходные уравнения для автомата $M_1^{'}$получаются из (6):

$$x_t = y_t + y_{t-1} + y_{t-2}y_{t-1},\ t \geq 0 \qquad (8)$$

Входо-выходная функция автомата $M_2^{'}$есть $f_1^{'}(z_{-1}z_0) = z_{-1}+z_0$, поэтому $M_2^{'} =< \{0,1\},\{0,1\},\{0,1\},\psi_2^{'},\varphi_2^{'} >$и таблицы функций$\psi_2^{'},\varphi_2^{'}$следующие:

Таблица 11. Функция перехода ψ'_2

	z_{-1}	
z_0	0	1
0	0	1
1	1	0

Таблица 12. Функция выхода φ'_2

	$x_{-2}x_{-1}$	
z_0	0	1
0	0	1
1	1	0

В автомате $M_1^{'(\tau_1)} =< \{0,1\},\{0,1\}^2 \times \{0,1\},\{0,1\},\psi_1^{'(\tau_2)},\varphi_1^{'(\tau_2)} >$функции $\psi_1^{'(\tau_2)},\varphi_1^{'(\tau_2)}$ задаются таблицами

Таблица 13. Функция перехода $\psi_1^{'(\tau_2)}$

	$y_{-2}y_{-1}i$							
y_0	000	010	100	110	001	011	101	111
0	001	011	101	111	001	111	001	101
1	001	011	101	111	011	101	011	111

Таблица 14. Функция выхода $\varphi_1^{'(\tau_2)}$

	$y_{-2}y_{-1}i$							
y_0	000	010	100	110	001	011	101	111
0	0	0	0	0	0	1	0	0
1	0	0	0	0	1	0	1	1

Автомат $M^{'} = M_2^{'} \times M_1^{'(\tau_2)} =< \{0,1\},\{0,1\} \times \{0,1\}^2 \times \{0,1,\dots,\tau_2,\{0,1\},\psi^{'},\varphi^{'} >$задается таблицами переходов и выходов

Таблица 15. Функция перехода ψ'

	$z_{-1}y_{-2}y_{-1}i$							
z_0	0000	0010	0100	0110	0001	0011	0101	0111
0	0001	011	0101	0111	0001	0111	0001	0101
1	1001	1011	1101	1111	1011	1101	1011	1111

Таблица 16. Функция перехода ψ' продолжение

	$z_{-1}y_{-2}y_{-1}i$							
z_0	1000	1010	1100	1110	1001	1011	1101	1111
0	1001	1011	1101	1111	1011	1101	1011	1111
1	0001	0011	0101	0111	0001	0111	0001	0101

Таблица 17. Функция выхода φ'

	$z_{-1}y_{-2}y_{-1}i$							
z_0	0000	0010	0100	0110	0001	0011	0101	0111
0	0	0	0	0	0	1	0	0
1	0	0	0	0	1	0	1	1

Таблица 18. Функция выхода φ' продолжение

	$z_{-1}y_{-2}y_{-1}i$							
z_0	1000	1010	1100	1110	1001	1011	1101	1111
0	0	0	0	0	1	0	1	1
1	0	0	0	0	0	1	0	0

Последовательность

$\alpha 1$= 0100100001100101011011000110110001101111

автомат M_fв состоянии $q=0111$зашифровывает в последовательность

β=1110110100110010000101100011011000110111

которую автомат M'в состоянии $q'=0110$расшифровывает в последовательност 0α.

Для программной реализации данного примера используем автоматное программирование в среде UniMod[4] и язык программирования Java. Ниже на рисунках 1 и 2 приведены схемы автомата M_f и граф переходов:

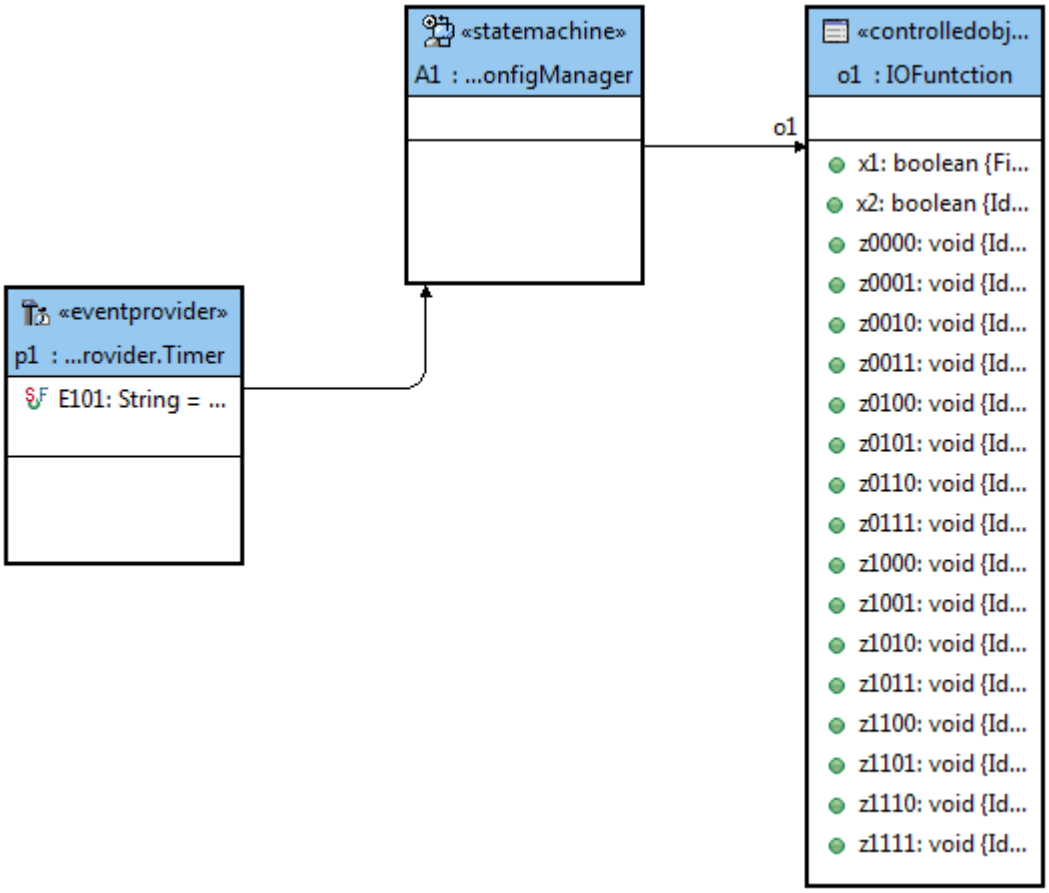

Рисунок 1. Схема автомата с функцией перехода ψ_f и функцией выхода φ_f

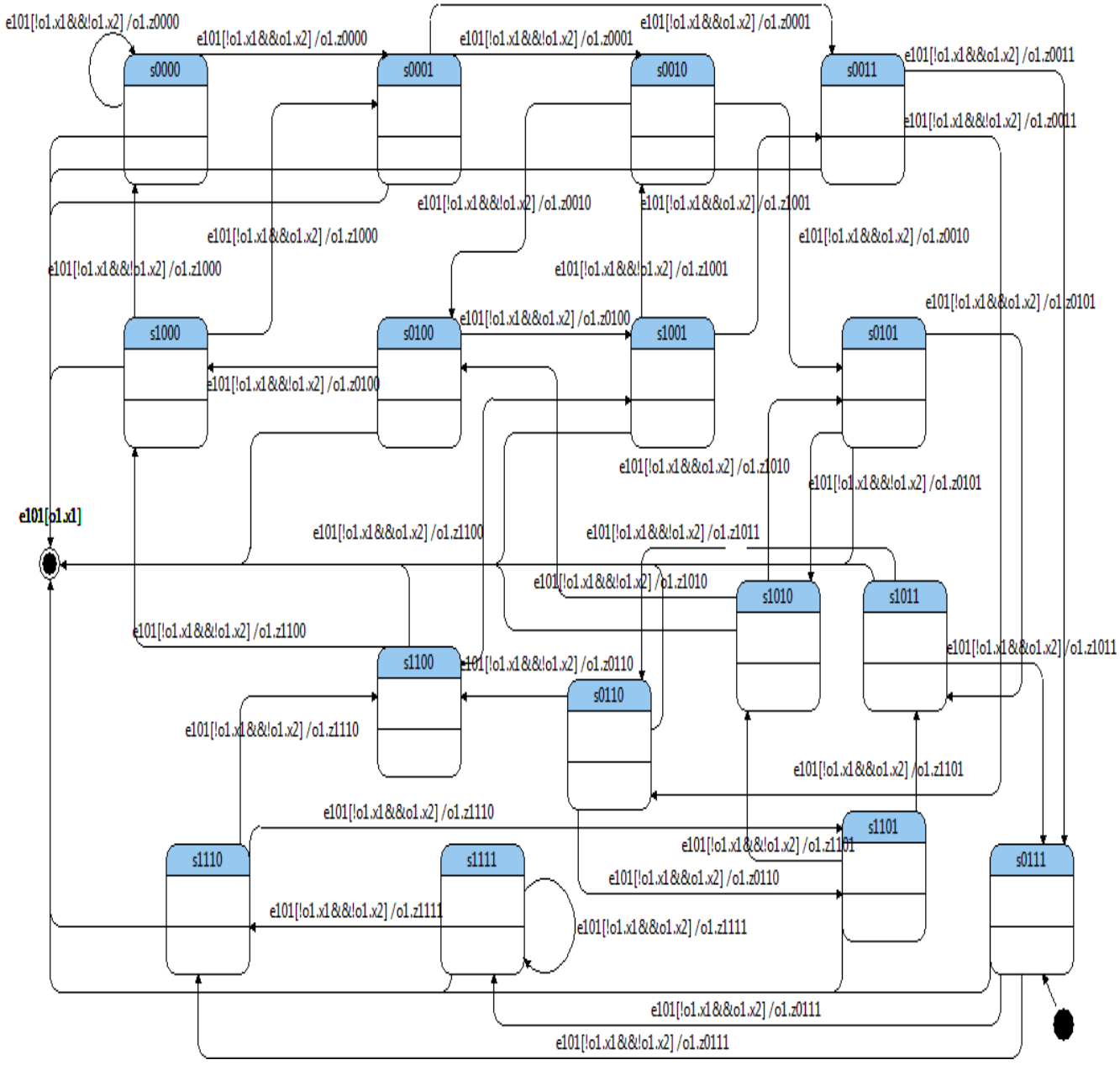

Рисунок 2. Графперехода автомата

В данном графе переходов условия и функции переходов определены следующим образом:

```
publicboolean x1(StateMachineContext context) {
        if(inputSqc.length()==i)returntrue;
        returnfalse;
        }

publicboolean x2(StateMachineContext context) {
        if((inputSqc.length()>i)&&inputSqc.charAt(i)=='1')
                returntrue;
        else
                returnfalse;
```

```
    }
publicvoid z0000(StateMachineContext context) {
    if(inputSqc.charAt(i)=='1'){
        outputSqc=outputSqc+"0";
        System.out.println("sub="+inputSqc.charAt(i)+"  i="+i);
        i=i+1;
        }
    else {
        outputSqc=outputSqc+"0";
        System.out.println("sub="+inputSqc.charAt(i)+"  i="+i);
        i=i+1;
        }
    }
```

Программа успешно протестирована для входной последовательности $\alpha 1$= 0100100001100101011011000110110001101111. Автомат дешифрование *M'* строится аналогичным образом.

Автоматное программирование базируется на теории автоматов и теории автоматического управления. В нашем случае само автоматное программирование использовано для реализации конечных автоматов. Как видно из рисунков 1 и 2 автоматное программирование можно рассматривать как программирование от состояний, что позволяет упростить процесс программирования конечных автоматов.

Список использованных источников

1. Tao R. J. Finite Automata and Application to Cryptography. – TSINGHUA University Press, 2009, 406 с.
2. Tao R. J., Chen S. H., Chen, X.M., FPKC3: A new Finite Automaton Public Key Cryptosystem // Laboratory for Computer Science №12, 1997, С. 289-305
3. Агибалов Г.П. Конечные автоматы в криптографии // Прикладная дискретная математика №2, 2009, С. 43-73.
4. Шалыто А.А. Автоматное программирование // Технические и программные средства систем управления, контроля и измерения, 2010

ӘӨК 004 432.4

ЖАЛҒАУЛАРДЫҢ ДҰРЫС ЖАЛҒАНУЫН АНЫҚТАУ

Сисенов Нурбек Маханбетулы
nurbek0692@gmail.com
«6М060200 - Информатика» мамандығының 2 курс магистранты, Астана, Қазақстан
Ғылыми жетекшісі - т.ғ.к Разахова Б.Ш.

Қазіргі жаһандану мен ақпараттандыру жағдайында кез келген табиғи тіл сол ортада даму үшін компьютерлік технологияларға ақпаратты өңдеу және жіберу, оны сақтау тілі ретінде кіруі керек. Сонымен қатар, дүниежүзілік компьютерлік желі Интернетте коммуникацияның тілі ретінде дамуы қажет. Адам тілін компьютерлік модельдеу интеллектуалды жүйені құру аймағындағы ең үлкен негізгі мәселелердің бірі болып табылады. Табиғи тілдік мәтіндер мен қолданушы арасындағы байланысты өңдеу, табиғи тіл негізіндегі үлкен базалық тілдік қорларды жинауды компьютерлік өңдеу секілді мәселелер компьютерлік желілердің күн өткен сайын көбеюіне байланысты үлкен өзектілікке ие. Сол себепті де бұл бағыт барлық дүниежүзінде қарқынды дамуда. Қазақстан Республикасының мемлекеттік тілі қазақ тілі үшін де маңызды болып табылады. Ол үшін қазақ тілінің жалғауларының дұрыс жалғануын зерттедік.