IDEA БЛОКЛИ ШИФРЛАШ АЛГОРИТМИНИ ТАКОМИЛЛАШТИРИШ МЕТОДЛАРИ

Равшонбек Отоназарович Султанов
Тошкент вилояти Чирчиқ давлат педагогика институти
E-mail: ravshanbek-1992@mail.ru

АННОТАЦИЯ

Мақолада AES шифрлаш алгоритмидан фойдаланган ҳолда IDEA8–1 тармоғига асосланган блоқли шифрлаш алгоритми келтирилган. Шифрлаш алгоритмида ишлатиладиган блоқлар узунлиги - 256 бит, раундлар сони - 10, 12 ва 14.

Калит сўзлар: шифрлаш, блоқ узунлиги, раундлар, калит, Фейстель тармоғи, Лай-Месси схемаси, AES, IDEA, дешифрлаш, SubBytes(), ShiftRows(), MixColumns(), AddRoundKey().

METHODS OF IMPROVING IDEA BLOCK ENCRYPTION ALGORITHM

ABSTRACT

The article presents the block encryption algorithm based on the IDEA8–1 network using the AES encryption algorithm. The length of the blocks used in the encryption algorithm is 256 bits, the number of rounds is 10, 12 and 14.

Keywords: encryption, block length, rounds, key, Feystel network, Lay-Messi scheme, AES, IDEA, decryption, SubBytes (), ShiftRows (), MixColumns (), AddRoundKey ().

КИРИШ

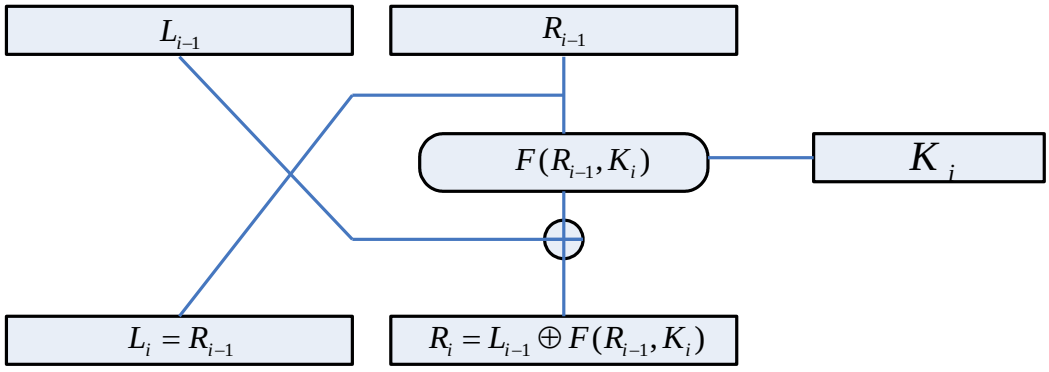
Симметрик блокли шифрлаш алгоритмлари бир нечта раундлардан иборат бўлиб, ҳар бир раунд аралаштирувчи ва тарқатувчи акслантиришлардан тузилган. Бундай асосда тузилиш тамойили, ҳар бир раунд шифрлаш жараёнини ҳар хил калитлар билан бир хил турдаги акслантиришларни амалга оширишга, ҳамда, дешифрлаш жараёнини раунд акслантиришлари ва калитларини тескари тартибда қўллашнинг самарали имконини беради.

Шифрланиши керак бўлган маълумот блокини силжитиш регистрларига киритиб, регистрдаги маълумотни шартли равишда чап ва ўнг қисмблок векторларига бўлиб, улар устида ҳар хил калитлар билан бир хил турдаги акслантиришларни босқичма-босқич амалга оширишга асосланган – *Фейстел*

тармоғи деб аталувчи шифрлаш жараёни функционал қурилмасига асосланган алгоритмлар кенг тарқалган.

АДАБИЁТЛАР ТАҲЛИЛИ ВА МЕТОДОЛОГИЯ

Фейстел тармоғининг қўлланиши кўпгина симметрик блокли шифрлаш алгоритмларида учрайди(1-расм). Бу алгоритмларга мисол қилиб LOCI, Khufu, Khafre, Blowfish, Lucifer, CAST, шунингдек, DES, ГОСТ 28147-89 каби стандарт алгоритмларни келтириш мумкин Фейстел тармоғи қуйидагича ифодаланади.



1-расм. Бир тармоқли Фейстел тармоғи структураси.

Блокли шифрлаш алгоритмлари яратишда Фейстел тармоғидан ташқари - *Лай–Мэсси схемасидан* ҳам фойдаланилади. PES, IDEA, MESH64, MESH96, MESH128, FOX, Akelarry каби шифрлаш алгоритмлари Лай–Мэсси схемаси асосида яратилган.[1]

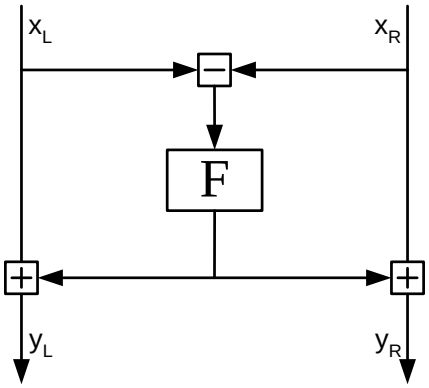
Лай–Месси схемасида шифрлаш қуйидагича амалга оширилади:

1. $\alpha_0 \leftarrow x_L$, $\beta_0 \leftarrow x_L$
2. $\alpha_{i+1} \leftarrow \sigma(\alpha_i + F(\alpha_i - b_i))$, $\beta_{i+1} \leftarrow \beta_i + F(\alpha_i - \beta_i)$,
3. $y_L \leftarrow \alpha_n$, $y_R \leftarrow \beta_n$

n–раундли Лай–Месси схемасини кўриб ўтсак(2-расм). F –раунд функция, H –акслантириш ва K_0, K_1, ..., K_n раунд калитлари бўлсин. Очиқ матн блоки L_0 ва R_0 қисмларга бўлинади. Ҳар бир раундда қуйидагича акслантиришлар амалга оширилади:

$$(L'_{i+1}, R'_{i+1}) = H(L'_i + T_i, R'_i + T_i),$$

бу ерда $T_i = F(L'_i - R'_i, K_i)$ ва $(L'_i, R'_i) = H(L_0, R_0)$. Шифрматн сифатида $(L_{n+1}, R_{n+1}) = (L'_{n+1}, R'_{n+1})$ қийматлар олинади.



2-расм. Лай-Месси схемаси структураси.

IDEA блокли шифрлаш алгоритми Лай–Месси схемасига асосланган. Алгоритм калит узунлиги 128 бит ва блок узунлиги 64 битга тенг, 8 раунд ва чиқувчи акслантиришдан иборат.

IDEA блокли шифрлаш алгоритми ҳозиргача бардошлилиги юқори бўлган алгоритмлар қаторига киради. Бардошлилигига ҳар хил арифметик амалларни аралаштириш ҳисобига эришилган. Раундларда 4 та кирувчи ва 4 та чиқувчи қисм блоклар ишлатилади.

НАТИЖАЛАР

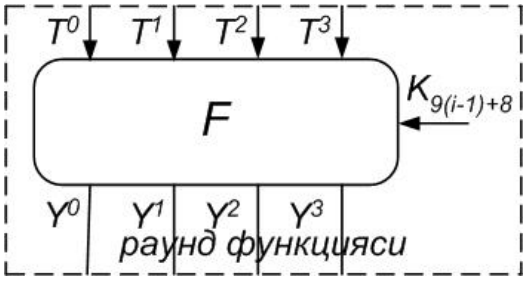
Бу алгоритмдан фойдаланиб раунд функцияси тўртта кириш ва чиқиш қисм блокига эга, битта раунд функциядан ташкил топган IDEA8–1 тармоғи ҳам яратиш мумкин. Агарда $T=[T^0,T^1,T^2,T^3]$ раунд функцияга кирувчи қисм блок, $Y=[Y^0,Y^1,Y^2,Y^3]$ раунд функциядан чиқувчи қисм блок сифатида қабул қилинса, тармоқ раунд функцияси $Y=F(T,K_{9(i-1)+8})$ кўринишда ифодаланади. Бу ерда

$$T^0=(X_{i-1}^0(z_0)K_{9(i-1)})\oplus(X_{i-1}^4(z_3)K_{9(i-1)+4}),$$

$$T^1=(X_{i-1}^1(z_1)K_{9(i-1)+1})\oplus(X_{i-1}^5(z_2)K_{9(i-1)+5}),\qquad T^2=(X_{i-1}^2(z_2)K_{9(i-1)+2})\oplus(X_{i-1}^6(z_1)K_{9(i-1)+6}),$$

$$T^3=(X_{i-1}^3(z_3)K_{9(i-1)+3})\oplus(X_{i-1}^7(z_0)K_{9(i-1)+7}).$$

Тармоқда $K_{9(i-1)}$, $K_{9(i-1)+1}$,..., $K_{9(i-1)+7}$, $i=\overline{1...n+1}$ раунд калитлари узунлиги 32 (16, 8) битга тенг бўлиб, F тармоқ раунд функциясига тўртта 32 (16, 8) битли блок кириб, тўртта 32 (16, 8) битли блок чиқади. $K_{9(i-1)+8}$, $i=\overline{1...n}$ раунд калити узунлиги 32 (16, 8) битга тенг бўлиши шарт эмас. Тармоқда барча раунд калитлар сони $9n+8$ га тенг бўлиб, раунд функциясида $K_{9(i-1)+8}$, $i=\overline{1...n}$ раунд калити, чиқувчи акслантиришда эса K_{9n}, K_{9n+1}, ..., K_{9n+7} раунд калитлари қўлланилган бўлиб, тармоқ раунд функцияси схемаси 3-расмда келтирилган.



3-расм.IDEA8–1 тармоғи раунд функцияси схемаси

Тармоқ шифрлаш фўрмуласига аниқлик киритиш мақсадида $Y = F(T, K_{9(i-1)+8})$ раунд функцияси $Y^0 = F^0(T^0, T^1, T^2, T^3, K_{9(i-1)+8})$, $Y^1 = F^1(T^0, T^1, T^2, T^3, K_{9(i-1)+8})$, $Y^2 = F^2(T^0, T^1, T^2, T^3, K_{9(i-1)+8})$, $Y^3 = F^3(T^0, T^1, T^2, T^3, K_{9(i-1)+8})$ кўринишда ифодаланади.[3],[9]

Бундан ташқари блокли шифрлаш алгоритмлари SPN тармоғига ва аралаш тармоққа асосланган бўлиши мумкин. Бу кўринишдаги алгоритмлари ичида AES FIPS 197 алгоритми энг машҳуридир.

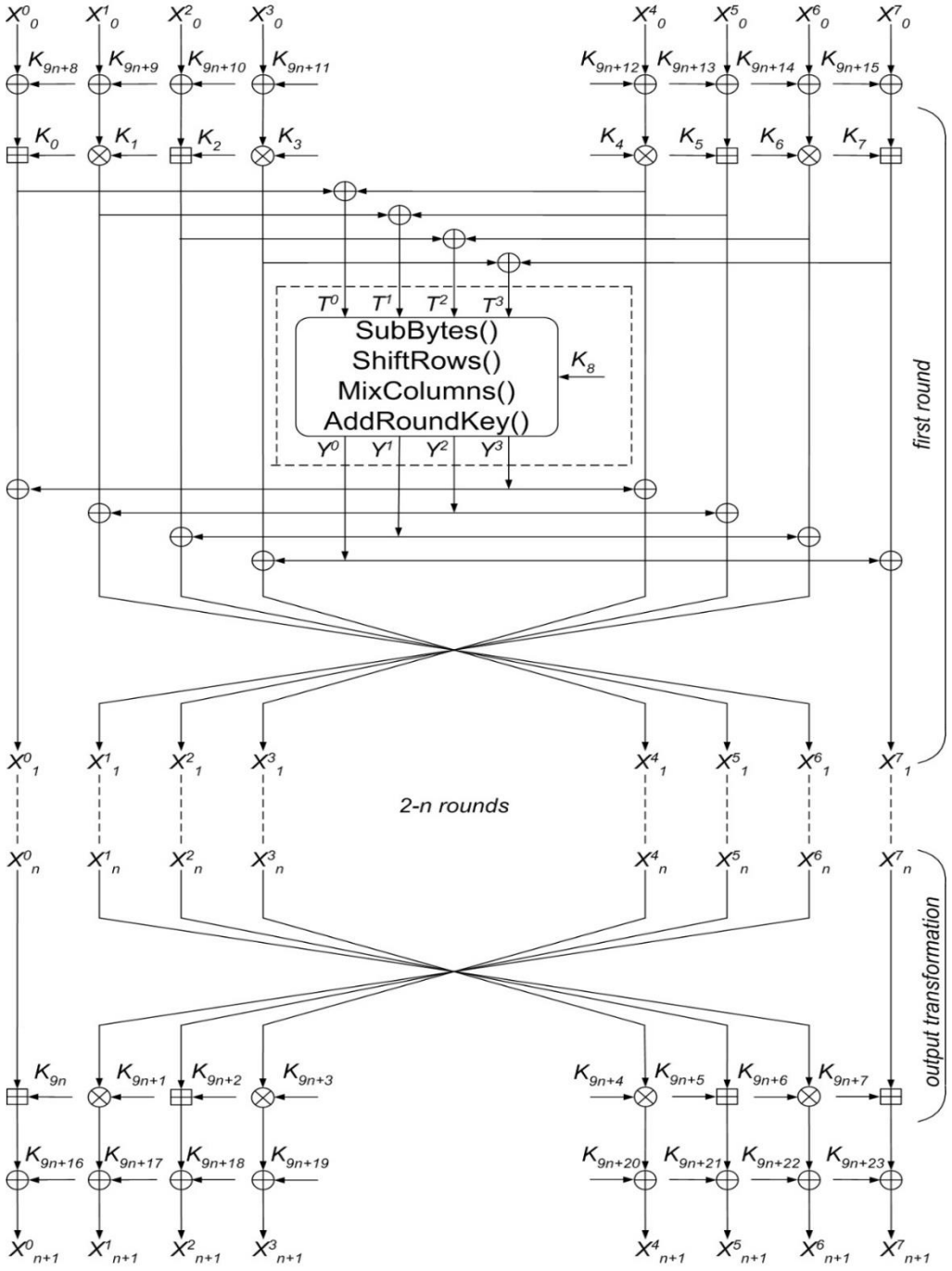
AES FIPS 197 блокли шифрлаш алгоритмида 8 ва 32-битли (1-байтли ва 4-байтли) векторлар устида амаллар бажарилади. AES FIPS 197 шифрлаш алгоритми XXI асрнинг энг барқарор шифрлаш алгоритми деб ҳисобланади. Бу алгоритм бошқа мавжуд стандарт симметрик шифрлаш алгоритмларидан фарқли ўлароқ, Фейстел тармоғига асосланмаган блокли шифрлаш алгоритмлари қаторига киради. Блокли шифрлаш алгоритмлари бардошлилиги жиҳатидан юқори кўрсаткичли алгоритмлар хисобланади.[8],[2]

AES блокли шифрлаш алгоритми АҚШ давлат стандарт шифрлаш алгоритми ҳисобланиб, квадрат архитектурасига асосланган. Бу блокли шифрлаш алгоритми раундлар сони *n*=10, 12 ва 14 га, блок узунлиги 128 битга ва калит узунлиги 128, 192, 256 битга тенг бўлиб, SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() акслантиришлари қўлланилган. Блокли шифрлаш алгоритмида 128 битли очиқ матн блоки 4x4 ўлчамли квадрат матрица элементлари, яъни State массиви элементлари сифатида қабул қилинади.[11]

AES блокли шифрлаш алгоритмининг ягона чизиқсиз акслантириши S блоклари ҳисобланиб, чизиқсизлиги юқорилиги билан ажралиб туради. Бу S блокнинг алгебраик чизиқсизлик даражаси $\deg = 7$, чизиқсизлиги $NL = 112$, чизиқли криптотаҳлил усулига нисбатан бардошлилиги $\lambda = 32/256$, дифференциал криптотаҳлил усулига нисбатан бардошлилиги $\delta = 4/256$, қатьий лавин эффекти критерийси (SAC) ва чиқувчи битлар боғлиқсизлиги критерийси (BIC) 8 га тенг.[6],[5]

МУҲОКАМА

AES блокли шифрлаш алгоритми SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() акслантиришларидан фойдаланилган ҳолда IDEA8–1 тармоғига асосланган AES–IDEA8–1 блокли шифрлаш алгоритми ишлаб чиқиш мумкин. AES–IDEA8–1 блокли шифрлаш алгоритмининг блок узунлиги 256 битга, раундлар сони $n = 10, 12, 14$ га тенг ва калит узунлиги 256 битдан 1024 битгача 128 бит қадам билан ўзгаради, яъни калит узунлиги 256, 384, 512, 640, 768, 896 ва 1024 битга тенг. Алгоритм қуйидагича структурага эга:



4–расм. n–раундли AES–IDEA8–1 блокли шифрлаш алгоритми структураси

AES–IDEA8–1 блокли шифрлаш алгоритми шифрлаш жараёнини кўриб ўтсак. Дастлаб 256 битли X очиқ матн блоки 32 битли X_0^0, X_0^1, …, X_0^7 қисм блокларга бўлинади ва қуйидаги кетма-кетликда амалга оширилади:[10]

1) X_0^0, X_0^1, …, X_0^7 қисм блокларга K_{9n+8}, K_{9n+9}, ..., K_{9n+15} раунд калитлари мос равишда XOR амали бўйича қўшилади, яъни $X_0^i = X_0^i \oplus K_{9n+8+i}$ $i = \overline{0...7}$.

2) X_{i-1}^0, X_{i-1}^1, …, X_{i-1}^7 қисм блокларга $K_{9(i-1)}$, $K_{9(i-1)+1}$, …, $K_{9(i-1)+7}$ раунд калитлари кўпайтирилади ва қўшилади, сўнгра 32 битли T^0, T^1, T^2, T^3 қисм блоклар ҳисобланади. Бу жараённи

$T^0 = (X_{i-1}^0 + K_{9(i-1)}) \oplus (X_{i-1}^4 \cdot K_{9(i-1)+4})$, $T^1 = (X_{i-1}^1 \cdot K_{9(i-1)+1}) \oplus (X_{i-1}^5 + K_{9(i-1)+5})$,

$T^2 = (X_{i-1}^2 + K_{9(i-1)+2}) \oplus (X_{i-1}^6 \cdot K_{9(i-1)+6})$, $T^3 = (X_{i-1}^3 \cdot K_{9(i-1)+3}) \oplus (X_{i-1}^7 + K_{9(i-1)+7})$, $i = 1$.

кўринишда ифодалаш мумкин.

3) T^0, T^1, T^2, T^3 қисм блоклар 8 битли t_0, t_1, ..., t_{15} қисм блокларларга бўлиб чиқилади ва SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() акслантиришлари бажарилади. Акслантиришлар натижасида 32 битли Y^0, Y^1, Y^2, Y^3 қисм блоклар ҳосил бўлади.

4) Y^0, Y^1, Y^2, Y^3 қисм блокларга X_{i-1}^0, X_{i-1}^1, …, X_{i-1}^7, қисм блоклар XOR бўйича қўшилади, яъни $X_{i-1}^j = X_{i-1}^j \oplus Y_{3-j}$, $X_{i-1}^{j+4} = X_{i-1}^{j+4} \oplus Y_{3-j}$, $j = \overline{0...3}$, $i = 1$.

5) раунд сўнггида X_{i-1}^0 ва X_{i-1}^7 блокдан ташқари барча қисм блоклар ўрин алмашади, яъни $X_i^j = X_{i-1}^{7-j}$, $j = \overline{0...7}$, $i = 1$.

6) 2-5 қадамлар n марта, яъни $i = \overline{2...n}$ марта такрорланади ва X_n^0, X_n^1, …, X_n^7 қисм блоклар ҳосил бўлади.

7) чиқувчи акслантиришда раунд калитлари қисм блокларга қўшилади ва кўпайтирилади, яъни $X_{n+1}^0 = X_n^0 + K_{9n}$, $X_{n+1}^1 = X_n^6 \cdot K_{9n+1}$, $X_{n+1}^2 = X_n^5 + K_{9n+2}$, $X_{n+1}^3 = X_n^4 \cdot K_{9n+3}$, $X_{n+1}^4 = X_n^3 \cdot K_{9n+4}$, $X_{n+1}^5 = X_n^2 + K_{9n+5}$, $X_{n+1}^6 = X_n^1 \cdot K_{9n+6}$, $X_{n+1}^7 = X_n^7 + K_{9n+7}$ қийматлар ҳисобланади.

8) X_{n+1}^0, X_{n+1}^1, …, X_{n+1}^7 қисм блокларга K_{9n+16}, K_{9n+17}, …, K_{9n+23} раунд калитлари мос равишда XOR амали бўйича қўшилади, яъни $X_{n+1}^j = X_{n+1}^j \oplus K_{9n+16+j}$, $j = \overline{0...7}$. X очиқ матн блокининг шифрматни сифатида $X_{n+1}^0 \| X_{n+1}^1 \| ... \| X_{n+1}^7$ блок олинади.[7]

ХУЛОСА

Фейстел тармоғига асосланган блокли шифрлаш алгоритмлари каби IDEA8–1 тармоғига асосланган блокли шифрлаш алгоритми бардошлилиги тармоқ раунд функцияси бардошлилигига узвий боғлиқ. Шунинг учун, IDEA8–1 тармоғи раунд функцияси сифатида бардошлилиги юқори бўлган AES блокли шифрлаш алгоритми AddRoundKey(), SubBytes(), ShiftRows(), MixColumns() акслантиришларини қўллаш орқали бардошлилиги нисбатан юқори бўлган AES–IDEA8–1 блокли шифрлаш алгоритмига эга бўлинади.

REFERENCES

1. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. –СПб.: БХВ-Петербург, 2009. – 576 с.
2. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланиши. – Т.: «Ўзбекистон маркаси», 2009. –424 б.
3. Lai X., Massey J.L. A proposal for a new block encryption standard //Advances in Cryptology – Proc. Eurocrypt’90, LNCS 473, Springer-Verlag, 1991, pp. 389-404.
4. Туйчиев Ғ.Н. IDEA–128 //ТАТУ хабарлари. –Тошкент, 2009. №3. 25–27 б.
5. Жданов О.Н., Золотарев В.В. Методы и средства криптографической защиты информатsii. СибГАУ. –Красноярск, 2007. – 217 с.
6. Туйчиев Г.Н. О сетях IDEA8–2, IDEA8–1 и RFWKIDEA8–4, RFWKIDEA8–2, RFWKIDEA8–1, разработанные на основе сети IDEA8–4 Узбекский математический журнал, –Ташкент, 2014, №3, 104–118 с.
7. Tuychiev G. New encryption algorithm based on network IDEA8-1 using of the transformation of the encryption algorithm AES IPASJ International Journal of Computer Science, 2015, Volume 3, Issue 1, pp. 1-6
8. Жўраева Н.В., Султанов Р.О., Абдуллаева С.А., Рахимжонова В.А. Systematization of uzbek language word combinations. Наука и Мир. Волгоград, 2020, 144-149б.
9. Султанов Р.О. Юсупов М.Р., IDEA шифрлаш алгоритмининг дастурий аппарат воситаларида қўлланилиши. Умумтаълим мактабларида аниқ фанларни ўқитиш методикаси” мавзусидаги илмий амалий анжуман материаллари. 2019 й.
10. Хуррамов А.Ж., Камолов Э.Р., Decision development of management problems of biotechnological systems at an uncertainty of environmental states using the mathematical statistics methods. European Journal of Research and Reflection in Educational Sciences. 2020 й, Page 212.
11. Ахмеджонов Д.Г. Устройство для создания подпочвенного экрана. //Журнал: “Сельскохозяйственные машины и технологии”, Москва, 2017, №1, с. 34-37

12. Akhmedov, B. A., & Khasanova, S. K. (2020). Public education system methods of distance in education in development of employees. *Journal of Innovations in Engineering Research and Technology*, *1*(1), 252-256.
13. Ахмедов, Б. А. (2020). Математические модели оценки характиристик качества и надежности программного обеспечения. *EURASIAN EDUCATION SCIENCE AND INNOVATION JOURNAL*, *3*(10), 97-100.
14. Гулбоев, Н. А., Дуйсенов, Н. Э., Ахмедов, Б. А., & Рахманова, Г. С. (2020). Модели систем управления электрическими сетями. *Молодой ученый*, *22*(312), 105-107.