ELECTRONIC DIGITAL SIGNATURE PROTOCOL ON THE BASIS OF ASYMMETRIC ENCRYPTION ALGORITHM BASED ON THE DIFFICULTY OF DISCRETE LOGARIFICATION AND MULTIPLICATION OF MATRIXES WITH A PARAMETER ON A FINAL FIELD

Sh. Sh. Akhmadaliev
Kokand State Pedagogical Institute

ANNOTATION

In article the report of the electronic digital signature on the basis of asymmetric algorithm of the enciphering based on complexity discrete taking the logarithm and multiplication of matrixes with parameter on a final field at which, in formation of the digital signature there is a possibility of a choice of any number from the signed is developed.

Keywords: matrix, parameter, multiplication, finite field, discrete logarithm, complexity, asymmetry, encryption, algorithm, electronic digital signature.

Traditional the work to conduct according to something information sign , that 's it _ information document status giving a signature put person that's it the document that the author is (responsible) . legal guarantees .

The development of information - communication and computer network technologies created the basis for the implementation of electronic document exchange . At the same time, the need to develop a method for determining the authenticity of a document and its author in electronic document exchange has arisen. Indeed, there are cases of non-recognition of the authenticity of a document for subjective reasons: it is claimed that the information or signature in the document is not authentic. Such issues are resolved on the basis of electronic digital signature (EDI).

Digital signature solves the following issues [1-3] :

–makes it possible to authenticate (determine the authenticity of) the electronic document source;

–provides a way to determine the integrity of a document based on its hash value;

–provides non-repudiation of the signature .

Currently, there are various methods (schemes) of ERI implementation, which can be divided into three groups:

1) digital signature system (scheme) based on symmetric encryption ;

2) system (scheme) based on public key encryption ;

3) a system (scheme) based on specially developed algorithms of digital signature formation and verification .

In this article , electronic information using symmetric encryption algorithms based on parametric matrix multiplication [4] :

-enable to ensure confidentiality;

–It is analyzed whether it can be applied to the solutions of cryptographic problems, such as the implementation of the solution of the problems of verifying the integrity of the information and ensuring its authentication, enabling the implementation of an electronic digital signature together with the given XF, and developing practical application methods and protocols.

There are two ways to implement the ERI protocol scheme using a public key (symmetric) encryption algorithm.

In the first way to ensure the ERI of an electronic information, it is possible to use the encrypted expression of this information using the secret key of the sender of the electronic information. In this case, the ERI is the same as the length of the data to be signed. In order to create such signed information - an electronic document - the information to be signed is encrypted with the private key of the signer. In that case, all users of the information and communication network can make sure of the correctness of this signature by decrypting the information encrypted with the public key of the author (owner) of the signature. If the decryption result is the same as the signed information, the electronic document is considered authentic, otherwise it is not authentic.

In the second method, a digital signature is calculated and together with the information to be signed, it is sent to the corresponding subscriber through an open information and communication network. The calculation of the digital signature is carried out with the secret key of the signer, depending on the value of the result (checksum, hash function) of mapping the initial information to a digital block. In this case, the length of the digital signature does not depend on the length of the information to be signed. Implementation of the digital signature with the private key of the signer, as in the first method, ensures that the authority to correctly form his digital signature is given only to the author of the signature. In turn, the signature verification algorithm is known to all users of the information and communication network, and its verification is carried out with the public key of the signature author.

The first method looks at the protocol scheme. Let each i -user and j -user of the information-communication network have their own and (k_j^o, k_j^M) key pairs according to the symmetric encryption algorithm E (for example: RSA, El-Gamal, etc.) . (k_i^o, k_i^M)

If the creator of the electronic document - information is M not confidential, she is without
1) user i executes the digital signature in this form: P

$$M \,||\, E_{k_i^M}(M) = M \,||\, P = M',$$

where M' -digitally signed information –is an electronic document.
sent to user j through an open information and communication network .
Having received the information, user j performs the following:
1) Signed M' - a digital signature $P = E_{k_i^M}(M)$ is separated from the data.
2) The k_i^o digital signature is decrypted by the public key of the author of the signature:

$$D_{k_i^o}(P) = D_{k_i^o}(E_{k_i^M}(M)) = M .$$

3) If the information obtained as a result of decoding the digital signature is the same as the signed information, then the electronic document is considered authentic, otherwise it is not authentic.

When the information to be signed is confidential:
1) User i creates a digital signature P in this form:

$$E_{k_j^o}[\, M \,||\, E_{k_i^M}(M)] = E_{k_j^o}[\, M \,||\, P] = M',$$

here M' - signed information - electronic document.
2) The electronic document is sent to user j through an open channel of the information and communication network .
Having received the signed secret information, user j performs the following:
Performs this decryption with its private key : k_j^M

$$D_{k_j^M}(M') = D_{k_j^M}(\, E_{k_j^o}[\, M \,||\, E_{k_i^M}(M)]) = M \,||\, E_{k_i^M}(M) = M'.$$

2) A M' digital signature is created from the information obtained as a result of decryption $P = E_{k_i^M}(M)$.

Performs decryption with the public key of the author of the digital signature : k_i^o

$$D_{k_i^o}(P) = D_{k_i^o}(E_{k_i^M}(M)) = M .$$

4) If the information obtained as a result of decoding the digital signature is the same as the signed information, then the electronic document is considered authentic, otherwise it is not authentic.
The second method looks at the protocol scheme. It is considered a digital signature, that is, the result of mapping the information into a digital block (checksum NY , hash function $H(M) = h$) is performed with the secret key of the signer. The protocol of ERI formation, transmission, reception and verification of digitally signed information is considered.

If the electronic document organizer M - information if not confidential, it is without:
1) user i executes the digital signature in this form: P

$$M \,||\, E_{k_i^M}(NY) = M \,||\, P = M',$$

where M' -digitally signed information –is an electronic document.
sent to user j through an open information and communication network .
Having received the information, user j performs the following:
1) Signed M' - a digital signature $P = E_{k_i^M}(NY)$ is separated from the data.

digital signature is decrypted with the public key of the author of the signature: k_i^o

$$D_{k_i^o}(P) = D_{k_i^o}(E_{k_i^M}(NY)) = M .$$

3) If the information obtained as a result of decoding the digital signature is the same as the signed information, then the electronic document is considered authentic, otherwise it is not authentic.

When the information to be digitally signed is confidential :
1) User i creates a digital signature P as follows:

$$E_{k_j^o}[\, M \,||\, E_{k_i^M}(NY)] = E_{k_j^o}[\, M \,||\, P] = M',$$

here M' - signed information - electronic document.
is sent to user j through an open channel of the information and communication network .

Having received the signed secret information, user j performs the following:
Performs this decryption with its private key : k_j^M

$$D_{k_j^M}(M') = D_{k_j^M}(E_{k_j^o}[M \,||\, E_{k_i^M}(NY)]) = M \,||\, E_{k_i^M}(NY) = M'.$$

2) A M' digital signature is created from the information obtained as a result of decryption $P = E_{k_i^M}(NY)$.

3) Performs decryption with the public key of the author of the digital signature : k_i^o

$$D_{k_i^o}(P) = D_{k_i^o}(E_{k_i^M}(NY)) = NY.$$

4) If the NY of the information obtained as a result of digital signature decryption is the same as the NY obtained as a result of digital signature decryption , then the electronic document is considered authentic, otherwise it is not authentic.
The disadvantage of the ERI based on the public key encryption algorithm is that there is only one possible digital signature corresponding to the given M -information. Because the checksum NY (M)= NY corresponding to the given M -data always has the same value as the calculation of the hash function $H(M) = H$ value is based on the keyless algorithm and always has the same expression as a result of encryption and decryption is divided. This situation makes it difficult to use such ERI algorithms.
Specially developed (created) ERI calculation formulation and its verification algorithms are free from the above-mentioned shortcomings. Because in these algorithms, the value of the hash function of the information to be signed, in addition to the secret key of the signer, a parameter chosen by the signer is also used in forming the ERI.
Below is a symmetric encryption algorithm [4] created based on the complexity of the solution of the problem of parameter multiplication of matrices and discrete logarithmization in a finite field together with the given XF, using a parameter chosen by the signer practical application methods and protocols will be developed for the implementation of electronic digital signature, verification of the integrity of information and solutions for ensuring its authentication .
$R_{il}^t = g^{x_{il}^t} \bmod p$ of R $^t{}_{mxn}$ -matrix are determined by calculation, where $\boldsymbol{x_{il}^t}$ - unknowns (may consist of bytes), i=1,...,m; l=1,...,n. Then (p, g, A $^t{}_{mxn}$, R $^t{}_{mxn}$) is the public key of the quaternion, and x_{il}^t - the unknowns are t - of the user are declared as secret key elements.

Cryptosystem j - user t- to user $M_{n\times m}$ - encrypts public information and sends it with a digital signature depending on its hash value as follows:
1. $M = M_{n\times m}$ - according to the algorithm of the hash-function of selected open data, its hash value is H ( ) M = H ($M_{n\times m}$)= $H_{n\times m}$ = H.
R -numeric signature j on this hash-value is formed by the user x_{il}^j's private key and a number chosen by him k_1:

a) $R^{jk_1} = R^{jk_1}{}_{m\times n} = g^{x_{il}^j + k_1} \bmod p$ matrix elements are calculated;

b) Encryption $A_{n\times m}^j$ is performed in the form ® $H = A_{n\times m}^j + H_{n\times m} + A_{n\times m}^j R_{m\times n}^{jk_1} H_{n\times m} (\bmod p) = P_{n\times m} =$ P and a digital signature is formed.

3. The information M to be signed and its digital signature are P combined to obtain M ||P = M' -extended electronic document.

4. By j randomly choosing a number known only to the user , the k elements of the matrix are calculated according to the public key of the $R \ = R^{tk}{}_{m\times n} = (R^{t}_{il})^{k} \bmod p = g^{kx^{t}_{il}} \bmod p$ t - user. $R^{t}{}_{m\times n}$

5. $A^{t}_{n\times m}$ By performing the encryption in the form $C_{n\times m} = (w_{n\times m}; d_{t} = g^{k} \bmod p; d_{p} = g^{k_1} \bmod p)$ $\circledR\ M'_{n\times m} = A^{t}_{n\times m} + M'_{n\times m} + A^{t}_{n\times m} R^{tk}_{n\times m} M'_{n\times m} (\bmod p) =$, a $w_{n\times m}$ triplet is sent as ciphertext.

cipher has received the t data $C_{n\times m} = (w_{n\times m}; d_{t}; d_{p})$ - the user performs the decryption as follows:

1. Using a t secret key $d_{t}^{x^{t}_{il}} \bmod p = g^{kx^{t}_{il}} \bmod p = D^{tk}_{il}$ known only to the user x^{t}_{il}, the values are calculated and the $D_{m\times n}$ matrix is generated.

2. Open is the matrix $A^{t}_{n\times m} = (I_{n\times n} + A^{t}_{n\times m} D^{tk}_{m\times n})^{-1}(-A^{t}_{n\times m}) \bmod p$ which is the parametric inverse of the key $(A^{t}_{n\times m})^{\backslash -1}$.

3. $R = D^{tk}_{n\times m}$ Decryption is performed by performing this value substitution operation:

$$(A^{t}_{n\times m})^{\backslash -1} \circledR\ w_{n\times m} = (I_{n\times n} + A^{t}_{n\times m} D^{tk}_{m\times n})^{-1}(-A^{t}_{n\times m}) \circledR\ (A^{t}_{n\times m} + M'{}_{n\times m} + A^{t}_{n\times m} R^{tk}_{m\times n} M'{}_{n\times m})(\bmod p) =$$

$$= (I_{n\times n} + A^{t}_{n\times m} R^{tk}_{m\times n})^{-1}(-A^{t}_{n\times m}) + (A^{t}_{n\times m} + M'{}_{n\times m} + A^{t}_{n\times m} R^{tk}_{m\times n} M'{}_{n\times m}) +$$

$$+ (I_{n\times n} + A^{t}_{n\times m} R^{tk}_{m\times n})^{-1}(-A^{t}_{n\times m})\, R^{tk}_{m\times n}\, (A^{t}_{n\times m} + M'{}_{n\times m} + A^{t}_{n\times m} R^{tk}_{m\times n} M'{}_{n\times m}) (\text{mod p}) =$$

$$= (I_{n\times n} + A^{t}_{n\times m} R^{tk}_{m\times n})^{-1}(-A^{t}_{n\times m})\, (I_{m\times m} + R^{tk}_{m\times n} A^{t}_{n\times m}) + A^{t}_{n\times m} + (I_{n\times n} + A^{t}_{n\times m} R^{tk}_{m\times n}) M'{}_{n\times m} +$$

$$+ (I_{n\times n} + A^{t}_{n\times m} R^{tk}_{m\times n})^{-1}(-A^{t}_{n\times m}) R^{tk}_{m\times n}\, (I_{n\times n} + A^{t}_{n\times m} R^{tk}_{m\times n}) M'{}_{n\times m} (\text{mod p})$$

If all the diagonal elements of the matrices in the expression of this last equality are non-zero, and all other elements are zero (such matrices have the property of commutativity), then the equality does not change even if they are exchanged in the terms involving matrix products. This equality holds for such matrices:

$$(A^{t}_{n\times m})^{\backslash -1} \quad \circledR \quad w_{n\times m} \quad = \quad (I_{n\times n} + A^{t}_{n\times m} R^{tk}_{m\times n})^{-1}(-A^{t}_{n\times m})\, (I_{m\times m} + R^{tk}_{m\times n} A^{t}_{n\times m}) + A^{t}_{n\times m} +$$

$$+ (I_{n\times n} + A^{t}_{n\times m} R^{tk}_{m\times n}) M'{}_{n\times m} + (I_{n\times n} + A^{t}_{n\times m} R^{tk}_{m\times n})^{-1}(-A^{t}_{n\times m}) R^{tk}_{m\times n}\, (I_{n\times n} + A^{t}_{n\times m} R^{tk}_{m\times n}) M'{}_{n\times m} \quad (\text{mod} \quad \text{p} \quad) =$$

$$(-A^{t}_{n\times m})(I_{n\times n} + A^{t}_{n\times m} R^{tk}_{m\times n})^{-1}\, (I_{m\times m} + R^{tk}_{m\times n} A^{t}_{n\times m}) + A^{t}_{n\times m} + \quad + \quad (I_{n\times n} + A^{t}_{n\times m} R^{tk}_{m\times n}) M'{}_{n\times m} +$$

$$(-A^{t}_{n\times m}) R^{tk}_{m\times n} (I_{n\times n} + A^{t}_{n\times m} R^{tk}_{m\times n})^{-1}\, (I_{n\times n} + A^{t}_{n\times m} R^{tk}_{m\times n}) M_{n\times m} \quad (\text{mod} \quad \text{p} \quad) \quad = \quad - A^{t}_{n\times m} + A^{t}_{n\times m} +$$

$$M'{}_{n\times m} + A^{t}_{n\times m} R^{tk}_{m\times n} M'{}_{n\times m} - A^{t}_{n\times m} R^{tk}_{m\times n}\ M'{}_{n\times m} (\text{ mod p}) = M'{}_{n\times m}.$$

In general, if the matrices participating in these equality expressions are chosen so that they have the property of commutativity, the decoding process mentioned above can be easily implemented. Here

$$M'{}_{n\times m} = M_{n\times m} \,||\, P_{n\times m} \text{ and } P_{n\times m} = A^{j}_{n\times m} + H_{n\times m} + A^{j}_{n\times m} R^{jk_1}_{m\times n} H_{n\times m} (\bmod p) = A^{j}_{n\times m} \circledR\ H = P$$

taking into account that the process of determining the correctness of the electronic digital signature continues as follows:

4. j - is $R^{j}_{m\times n}$ calculated by $D^{jk_1}_{n\times m}$ multiplying by the public $R^{jk_1}_{il} = g^{x^{j}_{il}+k_1} \bmod p = D^{jk_1}_{il}$ key of the user, the $d_p = g^{k_1} \bmod p$ -matrix is generated.

5. Open is the matrix $A^{j}_{n\times m} = (I_{n\times n} + A^{j}_{n\times m} D^{jk_1}_{m\times n})^{-1}(-A^{jk_1}_{n\times m}) \bmod p$ which is the parametric inverse of the key $(A^{j}_{n\times m})^{\backslash -1}$.

6. $R = D^{jk_1}_{n\times m}$ Decryption is performed by performing this value substitution operation:

$$(A^{j}_{n\times m})^{\backslash -1} ® \; w_{n\times m} = (I_{n\times n} + A^{j}_{n\times m} D^{jk_1}_{m\times n})^{-1}(-A^{j}_{n\times m}) ® \; (A^{j}_{n\times m} + H_{n\times m} + A^{j}_{n\times m} R^{jk_1}_{m\times n} H_{n\times m})(\bmod p) =$$

$$= (I_{n\times n} + A^{t}_{n\times m} R^{jk_1}_{m\times n})^{-1}(-A^{t}_{n\times m}) + (A^{t}_{n\times m} + H_{n\times m} + A^{t}_{n\times m} R^{jk_1}_{m\times n} H_{n\times m}) +$$

$$+ (I_{n\times n} + A^{j}_{n\times m} R^{jk_1}_{m\times n})^{-1}(-A^{j}_{n\times m}) \, R^{jk_1}_{m\times n} \, (A^{j}_{n\times m} + H_{n\times m} + A^{j}_{n\times m} R^{jk_1}_{m\times n} H_{n\times m}) (\mathrm{mod\ p}) =$$

$$= (I_{n\times n} + A^{j}_{n\times m} R^{jk_1}_{m\times n})^{-1}(-A^{j}_{n\times m}) \, (I_{m\times m} + R^{jk_1}_{m\times n} A^{j}_{n\times m}) + A^{j}_{n\times m} + (I_{n\times n} + A^{t}_{n\times m} R^{jk_1}_{m\times n}) H_{n\times m} +$$

$$+ (I_{n\times n} + A^{j}_{n\times m} R^{jk_1}_{m\times n})^{-1}(-A^{j}_{n\times m}) R^{jk_1}_{m\times n} \, (I_{n\times n} + A^{j}_{n\times m} R^{jk_1}_{m\times n}) H_{n\times m} (\mathrm{mod\ p})$$

Taking into account that only the diagonal elements of the matrices in the expression of this last equality are not zero, and all the other elements are zero (such matrices have the property of commutativity), using the fact that the equality does not change even if they are exchanged in the terms involving multiple expressions of the matrices, this equality has the equality:

$$(A^{j}_{n\times m})^{\backslash -1} \quad ® \quad w_{n\times m} \quad = \quad (I_{n\times n} + A^{j}_{n\times m} R^{jk_1}_{m\times n})^{-1}(-A^{j}_{n\times m}) \, (I_{m\times m} + R^{jk_1}_{m\times n} A^{j}_{n\times m}) + A^{j}_{n\times m} +$$

$$+ (I_{n\times n} + A^{j}_{n\times m} R^{jk_1}_{m\times n}) H_{n\times m} + (I_{n\times n} + A^{j}_{n\times m} R^{jk_1}_{m\times n})^{-1}(-A^{j}_{n\times m}) R^{jk_1}_{m\times n} \, (I_{n\times n} + A^{t}_{n\times m} R^{t}_{m\times n}) H_{n\times m} \quad (\quad \mathrm{mod} \quad \mathrm{p} \quad)=$$

$$(-A^{j}_{n\times m})(I_{n\times n} + A^{j}_{n\times m} R^{jk_1}_{m\times n})^{-1} \, (I_{m\times m} + R^{jk_1}_{m\times n} A^{j}_{n\times m}) + A^{j}_{n\times m} + \qquad + \qquad (I_{n\times n} + A^{j}_{n\times m} R^{jk_1}_{m\times n}) H_{n\times m} +$$

$$(-A^{j}_{n\times m}) R^{jk_1}_{m\times n} (I_{n\times n} + A^{jt}_{n\times m} R^{jk_1}_{m\times n})^{-1} \, (I_{n\times n} + A^{j}_{n\times m} R^{jk_1}_{m\times n}) H_{n\times m} \quad (\mathrm{mod} \quad \mathrm{p} \quad) \quad = \quad - A^{j}_{n\times m} + A^{j}_{n\times m} +$$

$$H_{n\times m} + A^{j}_{n\times m} R^{jk_1}_{m\times n} H_{n\times m} \; H_{n\times m} + A^{j}_{n\times m} R^{jk_1}_{n\times m} H_{n\times m} - A^{t}_{n\times m} R^{t}_{m\times n} \; H_{n\times m} (\mathrm{mod\ p}) = \; H_{n\times m} .$$

7. The part of the expanded document M_1 generated as a result of decryption of encrypted information by $M_1^{\prime}$ user $C_{n\times m}$ t is hashed: H (M_1)= H $M_1 \,||\, P_1()$ $M_{1n\times m} = H_1$

8. H_1= If H ($M_{1n\times m}$)= H = $_{n\times m}$ H , the electronic document is considered whole (authentic) and the authenticity of its electronic digital signature implies the authenticity of its source .

In the proposed ERI algorithm, in addition to the private key of the signer, a parameter chosen by the signer was also used. Therefore, this ERI algorithm has the same properties as ERI algorithms based on the formation and verification of a specially designed (created) digital signature calculation.

REFERENKES

1. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии: Учебное пособие, 2-е изд. –М.: Гелиос АРВ, 2002.-480 с.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 - 816 с.
3. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши – Тошкент, “Ўзбекистон маркаси”, 2009 – 434 бет.

4. Хасанов П.Ф., Акбаров Д. Е., Ахмадалиев Ш. Ш. Параметрли алгебра амалларидан фойдаланиб мавжуд ҳисоблаш мураккабликлари асосида янги асимметрик алгоритмлар яратиш усуллари. //Инфокоммуникации: Сети-Технологии-Решения. -1(9)/2009. -с. 31-35.
5. Siddikov I. M., Sh S. O. ABOUT ONE INNOVATION METHOD OF LOCALIZATION OF INDEPENDENT DIGITAL DEVICES //E-Conference Globe. – 2021. – С. 204-205.
6. Khaidarova, S. "Sql-expressions That Manage Transactions." JournalNX: 307-310.
7. Хонбобоев, Хакимжон Икромович, and Дилшод Улугбекович Султанов. "РУКОВОДСТВО НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТЬЮ СТУДЕНТОВ ПРИ ОБУЧЕНИИ ПРЕДМЕТАМ ИНФОРМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ." Актуальные научные исследования в современном мире 12-1 (2016): 63-65.
8. Хонбобоев, Хакимжон Октамович, Фозилжон Усибхонович Полатов, and Мухаммад-Анасхон Хакимжонович Икромов. "Tasviriy san’atni oqitishda interfaol metodlardan foydalanish." Молодой ученый 3-1 (2016): 22-23.
9. Shukhratovich, Shirinov Feruzjon. "The Field of Computer Graphics and Its Importance, Role and Place in The Information Society." Texas Journal of Multidisciplinary Studies 4 (2022): 86-88.
10. Muydinovich, Rasulov Inom. "The Role of Digital Technologies in Growing Secondary School Students to the Profession." Eurasian Scientific Herald 6 (2022): 137-142.
11. Muydinovich, Rasulov Inom. "The Role of Digital Technologies in Growing Secondary School Students to the Profession." Eurasian Scientific Herald 6 (2022): 137-142.
12. Йулдошев, Уткир, and Уктамжон Жуманкузиев. "Определение ведущих педагогических закономерностей и основополагающих принципов формирования информационной культуры детей школьного возраста." Общество и инновации 2.5/S (2021): 68-76.
13. Mamadjanova, S. V. "DESIGN FEATURES OF VIRTUAL LEARNING ENVIRONMENTS." European International Journal of Multidisciplinary Research and Management Studies 2.06 (2022): 1-5.
14. Toshpulatov, Raximjon I. "MODERN METHODS AND TENDENCIES IN TEACHING INFORMATION TECHNOLOGY." International Journal of Pedagogics 2.09 (2022): 43-46.
15. Jo‘rayev, M. (2022). Professional ta’lim jarayonida fanlararo uzvilik va uzliksizlikni ta’minlash o‘quvchilari kasbiy tayyorgarligining muhim omili sifatida. Zamonaviy dunyoda amaliy fanlar: Muammolar va yechimlar, 1(29), 43-46.
16. Shirinov F., Mamasoliyev A. A GENERAL DESCRIPTION OF THE HARDWARE AND SOFTWARE ENVIRONMENT USED TO ORGANIZE COMPUTER-BASED LEARNING PROCESSES //Euro-Asia Conferences. – 2021. – Т. 3. – №. 1. – С. 63-65.
17. Tokhirovna, Khakimova Yoqutkhon. "Stages Of Implementation Of Distance Learning In Higher Education." Texas Journal of Philology, Culture and History 1 (2021): 38-39.
18. Normatov, R. N., M. M. Aripov, and I. M. Siddikov. "Analysis Method of Structural-complex System Indicators by Decomposition Into Subsystems." JournalNX 7.04 (2021): 68-71.

19. Shirinov F., Mamasoliyev A. AN INTELLIGENT COMPUTER NETWORK-BASED LEARNING PROCESS MANAGEMENT SYSTEM //Euro-Asia Conferences. – 2021. – T. 3. – №. 1. – C. 55-57.

20. Juraev, M. M. (2022). The value of open mass competitions in the process of digitalization of extracurricular activities of schoolchildren. Web of Scientist: International Scientific Research Journal, 3(10), 338-344.