Foydalanilgan adabiyotlar ro‘yxati:

(1). Aleyev N.M., Tojiyev Sh.R. (2018). Sonlar nazariyasi va algebra. Toshkent, “O‘qituvchi” nashriyoti.

(2). Asqarov A.S. (2021). Olimpiada matematikasining asoslari. Sonlar nazariyasi va kombinatika. Toshkent, "Akademnashr".

(3). Hardy G.H., Wright E.M. (2008). An Introduction to the Theory of Numbers (6th ed.). Oxford University Press.

(4). Burton D.M. (2011). Elementary Number Theory (7th ed.). New York, McGraw-Hill.

(5). Rosen K.H. (2011). Elementary Number Theory and Its Applications (6th ed.). Pearson Education.

(6). Vinogradov I.M. (2004). Elements of Number Theory. Mineola, NY, Dover Publications.

(7). Andreescu T., Andrica D. (2007). Number Theory: Structures, Examples, and Problems. Boston: Birkhäuser.

(8). Sirojiddinov S.H. (1990). Sonlar nazariyasi. Toshkent: “O‘qituvchi” nashriyoti.

(9). Sivaramakrishnan,R. (1989). Classical Theory of Arithmetic Functions. New York: Marcel Dekker.

(10). Koblitz N. (1994). A Course in Number Theory and Cryptography (2nd ed.). New York: Springer-Verlag.

Mavlonov Alisher Bagbekovich (“UNICON.UZ” MCHJ, Kriptologiya maktabi boshlig‘i;
a.mavlonov@unicon.uz)

ISHLAB CHIQILGAN OCHIQ KALITLI SHIFRLASH ALGORITMIGA NISBATAN SHIFRLANGAN MATNGA ASOSLANGAN HUJUM USULINING MATEMATIK SHARHI

Annotatsiya. *Mazkur tadqiqotda ishlab chiqilgan ochiq kalitli asimmetrik shifrlash algoritmining shifrlangan matnga asoslangan hujumlarga bardoshliligi matematik jihatdan tahlil qilingan. Tadqiqotda shifrlangan matn va ochiq kalit asosida hosil bo‘ladigan tenglamalar sistemasi modellashtirilib, noma’lum parametrlar va mumkin bo‘lgan yechimlar fazosi o‘rganildi. Natijalar ochiq matnni tiklash uchun ko‘plab parametr variantlarini ko‘rib chiqish zarurligini va bu jarayon sezilarli hisoblash resurslarini talab qilishini ko‘rsatdi. Bitta blokni tiklash nazariy jihatdan mumkin bo‘lsa-da, butun xabarni tiklash uchun ushbu jarayonni har bir blok bo‘yicha takrorlash talab etiladi.*

Kalit so‘zlar: *kriptotahlil, algebraik hujum, nochiziq tenglamalar sistemasi, hisoblash murakkabligi.*

МАТЕМАТИЧЕСКИЙ АНАЛИЗ МЕТОДА АТАКИ НА ОСНОВЕ ШИФРОТЕКСТА НА РАЗРАБОТАННЫЙ АЛГОРИТМ ШИФРОВАНИЯ С ОТКРЫТЫМ КЛЮЧОМ

Аннотация. *В данном исследовании проведён математический анализ устойчивости разработанного алгоритма асимметричного шифрования с открытым ключом к атакам на основе шифротекста. В исследовании смоделирована система уравнений, формируемая на основе шифротекста и открытого ключа, а также изучены неизвестные параметры и пространство возможных решений. Результаты показали, что для восстановления открытого текста необходимо рассмотреть множество вариантов параметров, что требует значительных вычислительных ресурсов. Хотя теоретически восстановление одного блока возможно, для восстановления всего сообщения необходимо повторить данную процедуру для каждого блока.*

Ключевые слова: *криптоанализ, алгебраическая атака, система нелинейных уравнений, вычислительная сложность.*

MATHEMATICAL ANALYSIS OF A CIPHERTEXT-ONLY ATTACK METHOD AGAINST THE DEVELOPED PUBLIC-KEY ENCRYPTION ALGORITHM

Annotation. *This study presents a mathematical analysis of the resistance of the developed public-key asymmetric encryption algorithm to ciphertext-based attacks. A system of equations derived from the ciphertext and public key was modeled, and the unknown parameters and space of possible solutions were investigated. The results showed that recovering the plaintext requires considering numerous parameter combinations, which requires significant computational resources. Although the recovery of a single block is theoretically possible, recovering the entire message requires repeating this procedure for each block.*

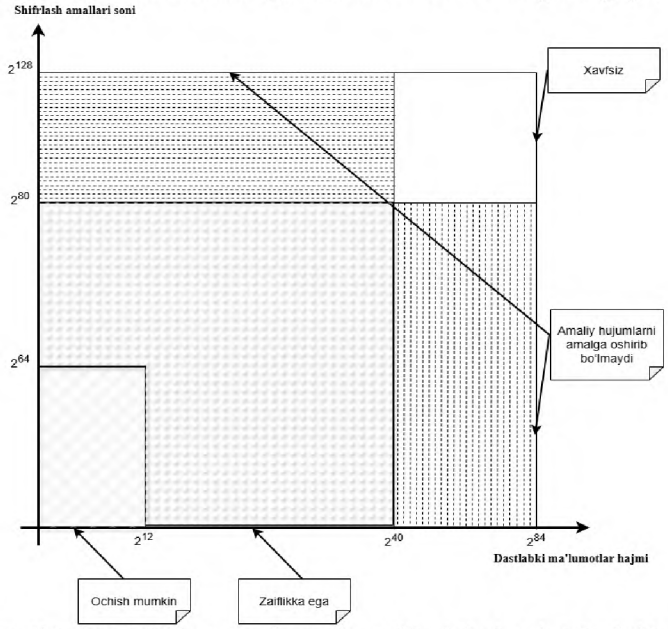
Keywords: *cryptanalysis, algebraic attack, system of nonlinear equations, computational complexity.*

I. Kirish. Kriptografiya doimiy o‘zgarishlarga uchraydigan soha bo‘lib, kuchli va ishonchli algoritmlar ishlab chiqish dolzarb masaladir. An’anaviy shifrlash usullari kuchayib borayotgan hisoblash imkoniyatlari va rivojlanib borayotgan hujum usullari bilan tobora ko‘proq tahdid ostida qolmoqda [1;536–539-b.; 2;665–670-b.]. Shu sababli innovatsion yechimlarga yangi ilmiy izlanishlarga tobora talab oshmoqda. Bugungi kunda yangi shifrlash algoritmlariga qo‘yiladigan asosiy talablar: ishonchlilik va kriptotahlilga bardoshlilik hisoblanadi. Shu sababli shifrlarning bardoshliligi har tomonlama tahlil qilinishi kerak.

Yopiq kalit uzunligi shifrning bardoshliligini baholashda muhim ahamiyatga ega. Kalit uzunligini oshirish hujumlarning ko‘p turlariga qarshi himoya qilishga yordam beradi. Shu bilan birga, kalitning ortiqcha uzunligi shifrlash tezligiga salbiy ta’sir ko‘rsatadi. Shu sababli tezkorlik va xavfsizlik o‘rtasidagi muvozanatni topish muhim hisoblanadi. So‘nggi yillarda kriptologiyaning barcha masalalari bo‘yicha ilmiy ishlarning juda jadal o‘sishini kuzatish mumkin. Jumladan, kriptologiyaning kriptotahlil yo‘nalishi juda izchillik bilan faol rivojlanayotgan tadqiqot sohasi hisoblanadi.

Kriptografik algoritmning bardoshliligi uni kriptotahlil uchun talab qilinadigan mehnat sarfi bilan belgilanadi. G‘araz niyatli tomonning intellektual va hisoblash imkoniyatlari turlicha bo‘lganligi sababli, shifrlash xavfsizligini ta’minlash uchun ishonchli chora-tadbirlar zarur. Kalit uzunligi, shifrlash tezligi va amalga oshirish qulayligi shifrlash tizimining samaradorligini baholashda muhim ahamiyatga ega [3;31–79-b.].

II. Mavzuga oid adabiyotlarning tahlili. Bugungi kunda zamonaviy EHM imkoniyatlari, talab etuvchi dastlabki ma’lumotlar va hisoblash resurslariga ko‘ra, ixtiyoriy kriptotahlil usulining amaliy ahamiyatini 1-rasmda tasvirlangan grafik asosida baholash mumkin [4;8–10-b.]. Shuni ham ta’kidlash lozimki, EHM imkoniyatlarining oshishi 1-rasmda tasvirlangan sohalar ko‘lamining kengayishiga ham olib keladi.



1-rasm. Turli kriptotahlil usullari amaliy qo‘llash imkoniyatlarini baholash.

Tarmoqlarda shifrlangan ma’lumotni uzatish jarayonida kriptotahlilchi: passiv yoki aktiv hujum turlarini amalga oshirishi mumkin [5;8–75-b.; 6;51–120-b.].

Passiv hujum maxfiy ma’lumotni aloqa tarmog‘ida uzatilayotganda eshitish, tahlil qilish, yozib olish kabi xatti-harakatlardan iborat bo‘lib, uzatilayotgan ma’lumot qabul qiluvchiga o‘zgarishsiz yetib boradi.

Aktiv hujum maxfiy ma’lumot uzatish jarayonini uzib qo‘yish, modifikatsiyalash, qalbaki shifr ma’lumotlar tayyorlash kabi xatti-harakatlardan iborat.

III. Tadqiqot metodologiyasi. Ishlab chiqilgan va [7;69–92-b.] adabiyotda to‘liq bayoni keltirilgan asimmetrik shifrlash algoritmi uchun quyidagi kriptohujum usullari ko‘rib chiqilishi mumkin:

Shifr matnga asoslangan hujumlar (Ciphertext-Only Attack). Bu usul kriptotahlil uchun eng kam ma’lumot sarfini tahlil qiladi: bunda shifrlangan ma’lumot ushlab olinadi va ochiq matnni, iloji bo‘lsa, yopiq kalitni topish ko‘zda tutiladi.

Ushbu usul eng murakkab hujum usullaridan biri hisoblansa-da, barcha zamonaviy kriptotizimlar, hech bo‘lmaganda, ushbu hujumni hisobga olgan holda ishlab chiqilgan bo‘lishi zarur [8;281–320-b.]. Agar al-goritm shifrlangan matnga asoslangan hujumga bardoshli bo‘lmasa, bu xabarlar yopiq kanallar orqali yu-borilishini anglatadi, bunday holda shifrlashga hojat qolmaydi.

Ma’lum ochiq matn asosidagi hujumlar (Known Plaintext Attacks). Ochiq va mos shifrlangan matn bloklari juftligi mavjud bo‘lgan holda algoritm tahlil qilinadi. Ma’lum bo‘lgan ochiq matn hujumi, hujumchiga shifrlangan matnni qo‘lga kiritganini va u bilan mos keladigan ochiq matnni bilishini va hujumchi yopiq kalitni olishni xohlayotganini bildiradi. Ma’lum bo‘lgan ochiq matn asosidagi hujum hali ham ko‘pchilik hollarda zarur hisoblanadi.

Algebraik hujumlar (Algebraic Attacks). Ushbu hujum asosida shifrlash tizimining matematik tuzilishini tahlil qilish va undagi algebraik masalalarni samarali yechish usullarini izlash yotadi. Algebraik hujumni amalga oshirishda hujumchi shifrlash yoki ochiq matn ma'lumotlariga asoslangan algebraik tenglamalar sistemalarini yechish orqali amalga oshiriladigan hujumlarga algoritmning bardoshligi ko'rib chiqiladi.

Algebraik hujumning samaradorligi ko'p jihatdan quyidagilarga bog'liq:

•tizimning tuzilishi. Kriptotizim murakkab algebraik amallarga, jumladan, chiziqsizlik xususiyatiga ega bo'lsa, hujum qiyinlashadi;

•tenglamalar soni va noma'lumlar soni. Agar noma'lumlar soni tenglamalar sonidan ortiq bo'lsa, hujumni amalga oshirish qiyinlashadi;

•hisoblash murakkabligi. Algebraik hujumlar odatda katta hisoblash resurslarini talab qiladi.

IV. Tahlil va natijalar. Endi yuqorida keltirib o'tilgan kriptotahlil usullarini ishlab chiqilgan algoritmga [7;69–92-b.] amaliy tatbiq qilinadi.

Shifrlangan matnga asoslangan hujum. Berilgan shifrlangan matnlar $(y^0, y^1, \dots, y^N)$ va ochiq kalit $K = S_{16\times16}, d_{3\times9}, \gamma_{8\times1}, \lambda_{6\times1}, \tau_{36\times1}, k_{2\times1}, \sigma, \Delta$ asosida biron bir ochiq matnni $\left(X^i, i = 0 \dots n\right)$ topishga urinish amalga oshiriladi. Bu yerda n – shifrlangan blokning tartibi.

$$
\begin{cases}
c_0 + k_0 c_1 = y_0 \\
(k_1 c_0 + c_1) \oplus \left(v_0 v_1 v_2 (modN)\right) = y_1 \\
\sigma\left(\sigma c_2 - (\lambda_0 x_7 + \sum_0^7 \gamma_i x_{i+8})\right)(modN) \oplus \left(not(v_0) v_1 v_2 (modN)\right) = y_2 \\
\sigma\left(c_2 + \sigma c_3 - (\lambda_1 x_7 + \gamma_7 x_8 + \sum_0^6 \gamma_i x_{i+9})\right)(modN) \oplus \left(not(v_1) v_0 v_2 (modN)\right) = y_3 \\
\sigma\left(\sum_2^3 c_i + \sigma c_4 - \left(\lambda_2 x_7 + \sum_6^7 \gamma_i x_{i+2} + \sum_0^5 \gamma_i x_{i+10}\right)\right)(modN) \oplus \left(not(v_2) v_0 v_1 (modN)\right) = y_4 \\
\sigma\left(\sum_2^4 c_i + \sigma c_5 - (\lambda_3 x_7 + \sum_5^7 \gamma_i x_{i+3} + \sum_0^4 \gamma_i x_{i+11})\right)(modN) \oplus \left(not(v_0 v_1) v_2 (modN)\right) = y_5 \\
\sigma\left(\sum_2^5 c_i + \sigma c_6 - (\lambda_4 x_7 + \sum_4^7 \gamma_i x_{i+4} + \sum_0^3 \gamma_i x_{i+12})\right)(modN) \oplus \left(not(v_0 v_2) v_1 (modN)\right) = y_6 \\
\sigma\left(\sum_2^6 c_i + \sigma c_7 - (\lambda_5 x_7 + \sum_3^7 \gamma_i x_{i+5} + \sum_0^2 \gamma_i x_{i+13})\right)(modN) \oplus \left(not(v_1 v_2) v_0 (modN)\right) = y_7 \\
\left(\frac{\Delta(\sum_2^7 c_i + \sigma c_8)(modN)}{p}\right) - (\sum_0^8 \tau_i x_{i+7})(modq) \oplus \left(not(v_1)\right) = y_8 \\
\left(\frac{(\sum_2^8 c_i + \sigma c_9)(modN)}{p}\right) - (\sum_9^{17} \tau_i x_{i-2})(modq) \oplus (v_1) = y_9 \\
\left(\frac{\Delta(\sum_2^9 c_i + \sigma c_{10})(modN)}{p}\right) + \sigma c_2 - (\sum_{18}^{26} \tau_i x_{i-11})(modq) \oplus \left(not(v_2)\right) = y_{10} \\
\left(\frac{(\sum_2^{10} c_i + \sigma c_{11})(modN)}{p}\right) + (c_2 + \sigma c_3) - \left(\sum_{27}^{35} \tau_i x_{i-20}\right)(modq) \oplus (v_2) = y_{11} \\
\left(\frac{\Delta(\sum_2^{11} c_i + \sigma c_{12})(modN)}{p}\right) + (\sum_2^3 c_i + \sigma c_4)(modq) = y_{12} \\
\left(\frac{(\sum_2^{12} c_i + \sigma c_{13})(modN)}{p}\right) + (\sum_2^4 c_i + \sigma c_5)(modq) = y_{13} \\
\left(\frac{\Delta(\sum_2^{13} c_i + \sigma c_{14})(modN)}{p}\right) + \left(\sum_2^5 c_i + \sigma c_6\right)(modq) = y_{14} \\
\left(\frac{(\sum_2^{14} c_i + \sigma c_{15})(modN)}{p}\right) + (\sum_2^6 c_i + \sigma c_7)(modq) = y_{15}
\end{cases}
\quad (1)
$$

(1) tenglamalar sistemasida noma'lum parametrlar bo'lib, $c_0, c_1, \dots, c_{15}$ va $x_7, x_8, \dots, x_{15}$ parametrlar hisoblanadi [7;69-92-b]. Tenglamalar sistemasi chiziqli emas. Bu tenglamalar sistemasini yechish uchun kriptotahlilchi $x_7, x_8, \dots, x_{15}$ parametrlarini tanlab olishi kerak bo'ladi. Bu shuni anglatadiki, ushbu tenglamalar sistemasi yagona yechimga ega emas, ya'ni 2^{352} mumkin bo'lgan yechim mavjud.

Shifrlash jarayonining navbatdagi almashtirishi [7;69–92-b.]da keltirilgan, $S_{16\times16}$ va $X_{16\times1}$ matritsalarini ko'paytirish bo'lib, bu (3) formula bilan ham shakl almashtirish mumkin.

$$C_{16\times1} = S_{16\times16} \cdot X_{16\times1}(modN) \quad (2)$$

yoki

$$
\begin{aligned}
\sum_0^6 s_{0i}x_i &= c_0 - \sum_7^{15} s_{0i}x_i \, modN \\
\sum_0^6 s_{1i}x_i &= c_1 - \sum_7^{15} s_{1i}x_i \, modN \\
\sum_0^6 s_{2i}x_i &= c_2 - \sum_7^{15} s_{2i}x_i \, modN \\
\sum_0^6 s_{3i}x_i &= c_3 - \sum_7^{15} s_{3i}x_i \, modN \\
\sum_0^6 s_{4i}x_i &= c_4 - \sum_7^{15} s_{4i}x_i \, modN \\
\sum_0^6 s_{5i}x_i &= c_5 - \sum_7^{15} s_{5i}x_i \, modN \\
\sum_0^6 s_{6i}x_i &= c_6 - \sum_7^{15} s_{6i}x_i \, modN \\
\sum_0^6 s_{7i}x_i &= c_7 - \sum_7^{15} s_{7i}x_i \, modN \\
\sum_0^6 s_{8i}x_i &= c_8 - \sum_7^{15} s_{8i}x_i \, modN \\
\sum_0^6 s_{9i}x_i &= c_9 - \sum_7^{15} s_{9i}x_i \, modN \\
\sum_0^6 s_{10i}x_i &= c_{10} - \sum_7^{15} s_{10i}x_i \, modN \\
\sum_0^6 s_{11i}x_i &= c_{11} - \sum_7^{15} s_{11i}x_i \, modN \\
\sum_0^6 s_{12i}x_i &= c_{12} - \sum_7^{15} s_{12i}x_i \, modN \\
\sum_0^6 s_{13i}x_i &= c_{13} - \sum_7^{15} s_{13i}x_i \, modN \\
\sum_0^6 s_{14i}x_i &= c_{14} - \sum_7^{15} s_{14i}x_i \, modN \\
\sum_0^6 s_{15i}x_i &= c_{15} - \sum_7^{15} s_{15i}x_i \, modN
\end{aligned}
\tag{3}
$$

(3) chiziqli tenglamalar sistemasida $x_0, x_1, \dots, x_6$ noma'lum parametrlar hisoblanadi. Chunki $x_7, x_8, \dots, x_{15}$ parametrlari tanlab olingan qiymatlarga ega. Bu shuni anglatadiki, (3) almashtirishlarning kirish parametrlari (1) almashtirishlarning kirish parametrlari bilan umumiylashtiriladi, ya'ni, shifrlash jarayonining ikkita almashtirishi o'rtasida teskari bog'liqlik tizimi mavjud.

Kriptotahlilchi 16 ta tenglama va 7 ta noma'lumdan iborat chiziqli tenglamalar tizimini oladi.

(3)da keltirilgan chiziqli tenglamalar sistemalarining yechimlarini topish uchun kriptotahlilchi [9; 120–170-b.] keltirilgan turli usullarni qo'llashi mumkin.

Tenglamalar sistemasini yechishda qo'llaniladigan usullardan qat'iy nazar, kriptotahlilchi quyidagicha harakatlarni bajaradi:

a) o'n oltitadan yettita tenglamani tanlaydi;

b) hosil bo'lgan tenglamalar sistemasini yuqorida keltirilgan usullardan biri yordamida yechiladi va $x_0, x_1, \dots, x_6$ parametrlarining qiymatlari olinadi;

d) olingan qiymatlarni qolgan tenglamalarga kiritadi va tengliklarning bajarilishini tekshiradi;

e) agar tenglik bajarilsa, kriptotahlilchi $x_0, x_1, \dots, x_{15}$ parametr qiymatlarini mumkin bo'lgan ochiq matn bloki sifatida qabul qiladi, aks holda, kriptotahlilchi yuqoridagi amallarni yana bajarishi kerak bo'ladi.

Natijada kriptotahlilchi 2^{800} ta mumkin bo'lgan variantlarni ko'rib chiqishi kerak bo'ladi, demak, ushbu holatda $x_0, x_1, \dots, x_{15}$ parametrlari uchun barcha mumkin bo'lgan variantlarni ko'rib chiqilishini anglatadi. Ulardan biri to'g'ri javob bo'ladi.

2^{800} ta mumkin bo'lgan variantlarini to'liq izlash natijasida, garchi amalda qiyin vazifa bo'lsa-da, kriptotahlilchi atigi 1 ta ochiq matn blokini qayta tiklay oladi. Qolgan ochiq matn bloklarini tiklash uchun kriptotahlilchi yuqoridagi amallarni yana takrorlaydi.

Agar ochiq matndagi bloklar soni n ga teng bo'lsa, unda ochiq matnni to'liq tiklash qiyinligi $n \times 2^{800}$ ga teng bo'ladi.

Yuqoridagilar shuni ko'rsatadiki, bunday turdagi hujumga ushbu algoritm bardoshli.

V. Xulosa. O'tkazilgan tadqiqotda ishlab chiqilgan ochiq kalitli asimmetrik shifrlash algoritmining shifrlangan matnga asoslangan hujumga bardoshliligi matematik jihatdan tahlil qilindi. Shifrlangan matn va ochiq kalit asosida hosil bo'ladigan tenglamalar sistemasi shakllantirilib, noma'lum parametrlarni aniqlash imkoniyati o'rganildi. Tahlil natijalari ochiq matnni tiklash uchun noma'lum parametrlarning ko'plab mumkin bo'lgan qiymatlarini tekshirish zarurligini va buning uchun sezilarli hisoblash resurslari talab etilishini ko'rsatdi. Ochiq matnni to'liq tiklash murakkabligi $n \times 2^{800}$ ga teng ekanligi va bu hozirgi hisoblash imkoniyatlarida imkonsiz ekanligi aniqlandi.

Foydalanilgan adabiyotlar ro'yxati:

[1]. Mavlonov A.B., Mavlonov A.B., Usb security and mechanism to ensure it. Science and innovation journal, Vol 2, Special Issue 3, 2023, p. 536–539 (12, Index Copernicus).

[2]. Mavlonov A.B. Vulnerability assessment and phishing analysis. International scientific and practical conference Smart technologies and innovative approaches in research: building a digital future, Ajou University in Tashkent, "Uzbekistan", February 22, 2025.
[3]. Koblitz N. "A Course in Number Theory and Cryptography" 2nd Edition, Springer-Verlag.
[4]. Kuryazov D.M., Sattarov A.B., Axmedov B.B. Blokli simmetrik shifrlash algoritmlari bardoshligina zamonaviy kriptotahlil usullari bilan baholash. Toshkent, "Aloqachi" nashriyoti, 2017.
[5]. Chuck Easttom. Modern Cryptography. Applied Mathematics for Encryption and Information Security. Mc Graw Hill Education, 2016.
[6]. Венбо Мао. Современная криптография. Теория и практика. Москва–Санкт-Петербург–Киев, Лори Вильямс, 2005.
[7]. Juraev G., Mavlonov A., A public key cryptosystem using matrix over the finite ring // Tatra mountains mathematical publications. 2025, t. 91, № 3.
[8]. Christopher Swenson. Modern Cryptanalysis. Techniques for Advanced Code Breaking. 1.1st Edition. January 23, 2022.
[9]. Фаддеев Д.К., Лекции по алгебре. Москва, «Наука», главная редакция, физико-математической литературы, 1984.

Nazarov Zuhriddin Akbar o'g'li ("Cyber university" davlat universiteti "Matematika va tabiiy fanlar" kafedrasi dotsenti; zuhrov13@gmail.com),
Iskandarov Sarvar Baltabayevich (Abu Rayhon Beruniy nomidagi Urganch davlat universiteti "Matematik tahlil" kafedrasi o'qituvchisi; sarvar.i@urdu.uz),
Ismoilova Munisa Orif qizi (Perfect University "Raqamli texnologiyalar" kafedrasi o'qituvchisi; munisaismoilova9718@gmail.com)

AXBOROT TIZIMLARIGA KIBERHUJUMLAR XAVFINI MARKOV ZANJIRLARI ASOSIDA MODELLASHTIRISH

Annotatsiya. *Zamonaviy sharoitda axborot tizimlariga qaratilgan kiberhujumlar sonining ortib borishi ularning xavfini miqdoriy baholash uchun ishonchli matematik vositalarni talab etadi. Mavjud tavsiyalar asosan sifatiy tavsifga tayanadi va tizim holatlarining vaqt bo'yicha dinamikasini yetarlicha aks ettirmaydi. Ushbu maqolada axborot tizimining xavfsizlik holatlari orasidagi o'tishlarni tavsiflovchi diskret vaqtli Markov zanjirlari asosida xavfni baholash modeli taklif etiladi. Tadqiqotda holatlar fazosi va o'tish ehtimolliklari matritsasi shakllantirilib, statsionar taqsimot hamda o'rtacha qaytish vaqti orqali xavf ko'rsatkichlari aniqlanadi. Model shartli sonli misolda sinovdan o'tkazilib, aniqlash ehtimolligining oshishi tizimning uzoq muddatli buzilish ehtimolligini qanday kamaytirishi ko'rsatib berilgan.*

Kalit so'zlar: *Markov zanjirlari, kiberhujum, xavfni baholash, o'tish ehtimolliklari matritsasi, statsionar taqsimot, stoxastik model, axborot xavfsizligi.*

МОДЕЛИРОВАНИЕ РИСКА КИБЕРАТАК НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ НА ОСНОВЕ ЦЕПЕЙ МАРКОВА

Аннотация. *В современных условиях рост числа кибератак на информационные системы требует надёжных математических инструментов для количественной оценки риска. Существующие рекомендации в основном опираются на качественное описание и недостаточно отражают динамику изменения состояний системы во времени. В данной статье предлагается модель оценки риска на основе дискретных цепей Маркова, описывающая переходы между состояниями безопасности информационной системы. В исследовании сформированы пространство состояний и матрица переходных вероятностей, на основе которых определяются показатели риска через стационарное распределение и среднее время возврата. Модель апробирована на условном числовом примере, показывающем, как повышение вероятности обнаружения снижает долгосрочную вероятность компрометации системы.*

Ключевые слова: *цепи Маркова, кибератака, оценка риска, матрица вероятностей переходов, стационарное распределение, стохастическая модель, информационная безопасность.*

MODELING THE RISK OF CYBERATTACKS ON INFORMATION SYSTEMS BASED ON MARKOV CHAINS

Annotation. *In modern conditions, the growing number of cyberattacks on information systems requires reliable mathematical tools for quantitative risk assessment. Existing guidelines are largely descriptive and do not adequately reflect the time dynamics of system state changes. This article proposes a risk-assessment model based on discrete-time Markov chains describing transitions between the security states of an information system. The study formalizes the state space and the transition probability matrix,*