MA’LUMOTLARNI HIMOYALASHDA KRIPTOTIZIMLARNING BARDOSHLI BO‘LISHILIGINI ZARURIYLIK KRITERIYSI

Umarov Sh.A.
Muhammad al-Xorazmiy nomidagi TATU Farg‘ona filiali

Ushbu maqolada axborotlarni himoya qilishda mumkin bo‘lgan tahdidlar, ma’lumotlar himoyalarini buzish sabablari, tashkilotlardagi axborot xavfsizligiga mas’ul shaxslarning vazifalari bayon qilingan. Shuningdek, axborot tizimini buzuvchining maqsadi tizimdagi zaifliklardan foydalanish va ma’lumotlarga ruxsatsiz kirish yoki tizimni o‘z manfaati uchun manipulyatsiya qilish usullari hamda zamonaviy kriptografik usullariga qo‘yiladigan umumiy talablar va keltirilgan. Ushbu talablar asosida kriptotizimlarning bardoshli bo‘lishiligini zaruriylik kriteriysi bayon qilingan.

Tayanch so‘zlar: kiberhujum, kriptotizim, autentifikatsiya, randomizator, algoritm immuniteti, kalitlarni boshqarish, kriptogramma.

В данной статье описаны возможные угрозы защите информации, причины нарушений защиты информации и обязанности лиц, ответственных за информационную безопасность в организациях. Также целью злоумышленника информационной системы является использование слабых мест системы и получение несанкционированного доступа к информации или манипулирование системой в корыстных целях, а также общие требования к современным криптографическим методам. На основе этих требований сформулирован критерий необходимости стойкости криптосистем.

Ключевые слова: кибератака, криптосистема, аутентификация, рандомизатор, устойчивость алгоритма, управление ключами, криптограмма.

This article describes possible threats to information security, causes of information security violations, and the responsibilities of those responsible for information security in organizations. Also, the goal of an information system attacker is to exploit the weaknesses of the system and gain unauthorized access to information or manipulate the system for personal gain, as well as general requirements for modern cryptographic methods. Based on these requirements, a criterion for the need for the strength of cryptosystem is formulated.

Keywords: cyberattack, cryptosystem, authentication, randomizer, algorithm stability, key management, cryptogram.

KIRISH

Axborotni himoya qilish bilan bevosita shug‘ullanmaydigan xodimlar axborot-kommunikatsiya tizimida ma’lumotlarni himoya qilish qoidalarining buzilishiga olib keladigan ko‘'plab sabablarni to‘liq tushuna olmasligi mumkin. Ma’lumotlar himoyasini buzishi mumkin bo‘lgan ba’zi umumiy sabablar [1]:

- Inson xatosi: tasodifiy ma’lumotlar sizib chiqishi, noto‘g‘ri sozlangan tizimlar yoki maxfiy ma’lumotlardan noto‘g‘ri foydalanish kabi shaxslar tomonidan qilingan xatolar.

- Insider tahdidlar: xodimlar yoki pudratchilar kabi maxfiy ma’lumotlarga ruxsatga ega bo‘lgan tashkilot ichidagi shaxslarning zararli harakatlari.
- Kiberhujumlar: xakerlar yoki kiberjinoyatchilarning zararli harakatlari, jumladan, fishing, zararli dastur, to‘lov dasturi yoki tizimdagi zaifliklardan foydalanish.
- Zaif xavfsizlik choralari: zaif parollar, shifrlashning yo‘qligi yoki eskirgan dasturiy ta’minot kabi xavfsizlikni boshqarishning etarli emasligi ruxsatsiz kirishni osonlashtiradi.
- Uchinchi tomon xavflari: maxfiy ma’lumotlarga kirish huquqiga ega bo‘lgan uchinchi tomon ishlab chiqaruvchilari yoki xizmat ko‘rsatuvchi provayderlar orqali ma’lumotlar buzilishi sodir bo‘lishi mumkin.
- Jismoniy o‘g‘irlik yoki yo‘qotish: Noutbuklar, smartfonlar yoki maxfiy ma’lumotlarni o‘z ichiga olgan xotira vositalari kabi qurilmalarning o‘g‘irlanishi yoki yo‘qolishi.
- Reglamentga muvofiqlik: ma’lumotlarni himoya qilish qoidalari va standartlariga rioya qilmaslik, bu jarima yoki huquqiy oqibatlarga olib kelishi mumkin.
- Ijtimoiy muhandislik: maxfiy ma’lumotlarni oshkor qilish yoki ruxsatsiz kirishga ruxsat berish uchun shaxslarni aldash uchun ishlatiladigan manipulyatsiya usullari.

Tashkilotlar va jismoniy shaxslar ushbu potentsial xavflardan xabardor bo‘lishlari va ma’lumotlarni himoya qilish va ma’lumotlarni himoya qilish qoidalariga rioya etilishini ta’minlash uchun tegishli choralarni ko‘rishlari juda muhimdir.

MATERIALLAR VA USULLAR

Kriptografiya ma’lumotlarni himoya qilishda muhim rol o‘ynaydi va shuning uchun ma’lumotlarni himoya qilishda kriptografiya talablari bo‘yicha ko‘plab adabiyotlar mavjud. Jumladan: B.Shnayerning "Amaliy kriptografiya" – bu adabiyotdada muallif kriptografiya asoslari va uning ma’lumotlarni himoya qilishda qo‘llanilishini baton qilgan qilgan [2]. Shuningdek, u maxfiylik, yaxlitlik va autentifikatsiya kabi turli kriptografiya talablarini keltirib o‘tgan javob beradi. Uilyam Stallingning “Kriptografiya va tarmoq xavfsizligi” adabiyotida muallif tarmoq xavfsizligi kontekstida kriptografiyaga qo‘yiladigan talablar batafsil ko‘rib chiqilgan [3]. U turli xil shifrlash, autentifikatsiya va kalitlarni boshqarish algoritmlarini tahlil qilgan. Jonatan Katz, Yoav Shneidman muallifligidagi "Zamonaviy kriptografiyaga kirish" adabiyotida zamonaviy kriptografiyaga kirish bayon qilingan va maxfiylik, yaxlitlik va mavjudlik kabi ma’lumotlar xavfsizligi talablari o‘rganilgan [4]. Duglas Stiglitzning "Kriptografiya: nazariya va amaliyot" kitobida muallif kriptografiyaning nazariy asoslari va ma’lumotlarni himoya qilishda amaliy qo‘llanilishini keltirib o‘tgan. Shuningdek, u zamonaviy texnologiyalar va tahdidlar kontekstida kriptografiya talablarini tahlil qilgan [5]. Ushbu va boshqa ishlar ma’lumotlarni himoya qilishda kriptografiyaga qo‘yiladigan talablarni keng qamrovli o‘rganishni anglatadi va ular axborot xavfsizligi sohasidagi mutaxassislar uchun, shuningdek, ushbu mavzuga qiziqqan har bir tadqiqotchi uchun foydali bo‘lishi mumkin.

Muammo maqsadi korxonada axborotni himoya qilishda kriptotizimlarga qo‘yiladigan talablarni aniqlashdan iborat. Bunda korxonadagi axborot xavfsizligi ma’sullari oldida bir qator masalalar yuzaga keladi:

- Korxonadagi axborot konfidensialligi: ma’lumotlarni ruxsatsiz kirishdan himoya qilish, har xil turdagi ma’lumotlar turli darajadagi maxfiylik;
- Autentifikatsiya va ma’lumotlar yaxlitligi;
- Xavfsizlik talablariga javob beradigan kalit uzunligi miqdorini hisoblash;
- Shifrlash kalitlarini boshqarish va yangilash, asosiy ma’lumotlarni saqlash va uzatish texnologiyalari;
- Hisoblash va kriptoanalitik imkoniyatlarning mumkin bo‘lgan rivojlanishini hisobga olgan holda uzoq muddatda axborotni himoya qilish xavfsizligini kafolatlash.

Ma’lumotlarni himoya qilish qoidalarini buzuvchining maqsadi tizimdagi zaifliklardan foydalanish va ma’lumotlarga ruxsatsiz kirish yoki tizimni o‘z manfaati uchun manipulyatsiya qilishdir. Quyida ushbu maqsadlarni amalga oshirish uchun keng tarqalgan usullardan foydalaniladi [6]:

1) Ma’lumotlarga ruxsatsiz kirish: qoidabuzar xavfsizlik choralarini chetlab o‘tib, maxfiylik qoidalarini buzgan holda maxfiy ma’lumotlarni olish va unga egalik qilishni maqsad qilgan.

2) O‘zini namoyon qilish va ruxsatsiz foydalanish: qoidabuzar o‘zini vakolatli shaxs sifatida ko‘rsatib, o‘z vakolatiga kirish, yolg‘on ma’lumotlarni tashkillashtirish, haqiqiy ma’lumotlarni o‘zgartirish yoki ruxsatsiz ma’lumotlarni olish uchun o‘zini boshqa foydalanuvchi sifatida ko‘rsatishi mumkin.

3) Mavjud ma’lumotlarni tartibga solishni rad etish: qoidabuzar mavjud ma’lumotlarni tartibga solish yoki boshqarishni qasddan rad qilishi mumkin, bu esa ma’lumotlarning buzilishi yoki yo‘qolishiga olib kelishi mumkin.

4) Noto‘g‘ri ma’lumot: qoidabuzar noto‘g‘ri ma’lumot boshqa foydalanuvchi tomonidan uyushtirilgan deb noto‘g‘ri da'vo qilishi mumkin, bu esa javobgarlikni o‘z zimmasiga yuklashi yoki chalkashliklarni keltirib chiqarishi mumkin.

5) Yuborilgan ma’lumotni manipulyatsiya qilish: qoidabuzar ma’lumotlarning yuborilganligini noto‘g‘ri ko‘rsatishi, jo‘natish vaqtini noto‘g‘ri ko‘rsatishi yoki ma’lumotlarni olish faktini rad etishi mumkin.

6) Ruxsatsiz tarqatish va o‘zgartirish: qoidabuzar foydalanuvchilarga berilgan ruxsat etilgan ma’lumotlarni noqonuniy ravishda tarqatishi yoki kengaytirishi yoki ruxsatisiz foydalanuvchi ruxsatini o‘zgartirishi mumkin.

7) Maxfiylikni noto‘g‘ri ko‘rsatish: Buzg‘unchi maxfiy ma’lumotlarni maxfiy bo‘lmagan ma’lumotlar sifatida noto‘g‘ri ko‘rsatishi mumkin va bu maxfiy ma’lumotlar xavfsizligiga putur etkazishi mumkin.

8) Ruxsatsiz ulanish va axborot almashish: qoidabuzar aloqa tarmoqlariga ruxsatisiz ulanishi, boshqa tizimlardan muntazam ravishda axborot olishi va tarqatishi mumkin.

9) Axborot oqimini tahlil qilish: qoidabuzar aloqa kanallaridagi axborot oqimini tahlil qilishi, uni zararli maqsadlarda o‘rganishi va tizimdagi zaifliklardan foydalanishi mumkin.

10) Protokol maxfiyligini buzish: Buzuvchi protokolning yaxlitligiga shubha qilishi va protokolga muvofiq maxfiy bo‘lishi kerak bo‘lgan ma’lumotlarning maxfiyligini buzishi mumkin.

11) Ma’lumotlarni himoya qilish algoritmlarini o‘zgartirish: qoidabuzar ma’lumotlarni himoya qilish algoritmi dasturiga aniqlanmasdan, tizim xavfsizligiga putur etkazadigan o‘zgartirishlar kiritishi mumkin.

12) Rag‘batlantiruvchi qoidabuzarliklar: qoidabuzar boshqa foydalanuvchilarni yolg‘on ma’lumotlar yoki chalg‘ituvchi taktikalar asosida himoya protokolini buzishga undashi mumkin.

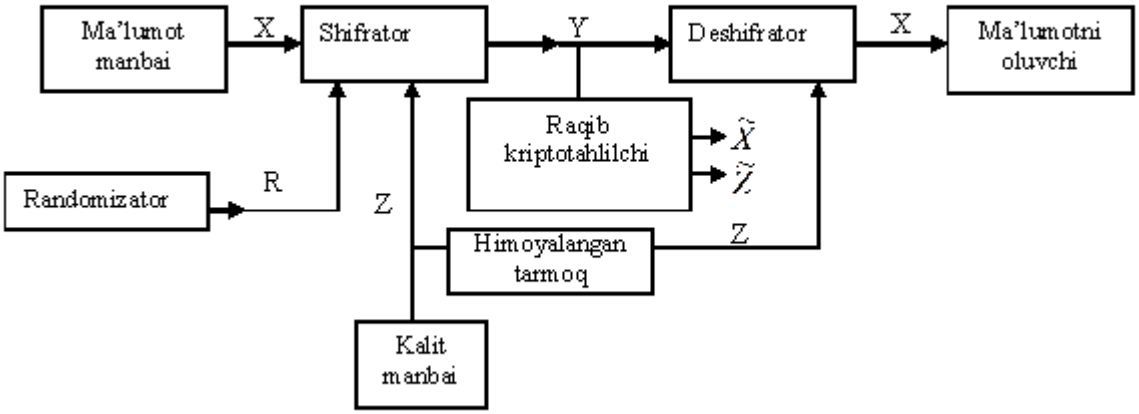
13) Ishonchni yo‘qotishga olib keladigan harakatlar: Buzg‘unchi tizim xavfsizligi va yaxlitligiga ishonchni yo‘qotishiga olib keladigan himoya protokolini buzadigan harakatlarni amalga oshirishi mumkin.

14) Axborot uzatishga xalaqit berish: qoidabuzar ma’lumotlarning sifatli uzatilishiga xalaqit berish uchun texnik, dasturiy ta’minot yoki boshqa usullardan foydalanishi mumkin, bu esa uzatilgan ma’lumotlarning haqiqiyligi va yaxlitligiga shubha uyg‘otadi.

Muammo maqsadi - muayyan xavfsizlik, ishlash va tartibga soluvchi talablarga muvofiqlik talablarini hisobga olgan holda korxonada ishonchli ma’lumotlarni himoya qilishni ta’minlaydigan kriptotizimlarga qo‘yiladigan talablarni aniqlash.

NATIJA VA MUHOKAMALAR

Ma’lumotlarni kriptografik uslublar bilan muhofazalash jarayonlari algoritmik tillar bilan maxsus kriptobardoshli algoritmlarni dasturlash orqali yoki maxsus texnik apparatlar yordamida amalga oshiriladi. Bunda dasturlash uslublari o‘zining qo‘llanilishi jihatidan qulayligi bilan ajralib turadi. Texnik apparatlardan foydalanish uslublari katta qiymatdagi moddiy mablag‘ni talab qilsada, o‘zining samaradorligi, qulayligi, ishonchliligi va shu kabi xususiyatlari bilan farqlanadi. 1-rasmdagi sxema Shennonning «Maxfiy tizimlarda aloqa nazariyasi» kitobida keltirilgan va shifrlash jarayoniga “randomizator” tushunchasi kiritilgan. Randomizatsiya autentifikatsiya masalalarida muhim o‘rin tutadi [7].



1- rasm. Ma’lumotlarni kriptografik uslublar bilan muhofazalash jarayoni.

Shu narsa muhimki, *X*, *Y* va *Z* – miqdorlarni tasodifiy deb tushunish kerak. Bunda ochiq matnning statistik xossalari ma’lumotlar manbai bilan aniqlanadi,

maxfiy kalit *Z* va randomizatsiyalash ketma-ketligi *R* miqdorlarning statistik xossalari kriptografga ma’lum. 1 - rasmda keltirilgan sxemaga asosan, *X*, *Z* va *R* miqdorlar statistik nuqtai nazardan bog‘liq emas. Kriptotahlilchi faqat uzatilayotgan ma’lumotning *Y*-kriptogrammasiga ega bo‘lgan holda *X* - ochiq ma’lumotni ochishga urunib, *Z* - maxfiy kalitning biror $\widetilde{Z}$ ko‘rinishdagi ifodasini va unga ko‘ra ochiq ma’lumotning biror $\widetilde{X}$ ko‘rinishini oladi.

K.Shennonning kriptografiyaga qo‘shgan hissasi kriptografik tizimlarning bardoshliligi uchun asosiy tamoyillar va shartlarni kiritishdan iborat bo‘lgan. Bunda entropiya hisoblanishi muhim hisoblanadi. Diskret signalning *N* ta mumkin bo‘lgan holatga ega entropiyasi quyidagicha hisoblanadi [8]:

$$H(x)=-\sum_{i=1}^{N} p(i)\log p$$

bu yerda $p(1), p(2),\ldots, p(N)$ qiymatlar $x_1, x_2,\ldots, x_N$ alifbo elementlarining paydo bo‘lish ehtimoli.

Ideal kriptobardoshli (mutlaqo, nazariy jihatdan aniqlab bo‘lmaydigan) tizim mavjudligi uchun zarur shartlar [9]:

1. Agar biron bir kriptogramma ushbu kriptogrammada shifrlangan ma’lumotni haqidagi ma’lumotni qo‘shmasa, tizim mutlaqo xavfsizdir.

$$I(E,M)=0,$$

bu yerda *I* – ma’lumotlar soni, *E* – kritogramma, *M* – xabar matni.

Kalitni bilmagan holda kriptogrammani ushlab olishda ma’lumot miqdori nolga teng.

$$I(E,M)=H(M)-H(M/E),$$

bu yerda *H*(*M*) – xabar manbasining entropiyasi, *H*(*M/E*) – kriptogramma ushlangan bo‘lsa, xabarning shartli entropiyasi.

2. Kalitlar soni xabarlar sonidan kam bo‘lmasligi kerak

$$L^N \geq m^n$$

bu yerda *L* – kalit ma’lumotining alifbo hajmi, *N* – kalit uzunligi, *m* – xabar alifbo hajmi, *n* – xabar uzunligi.

3. Kalit uzunligi xabar uzunligidan kam bo‘lmasligi kerak. Tengsizlikning har ikki tarafi logarifmlab yuboriladi:

$$\log L^N \geq \log m^n$$

Bundan kalit uzunligi ushbu ifoda bilan hisoblanadi

$$N \geq \frac{n\log m}{\log L}$$

Shunday qilib, agarda $L_X = L_Z$ bo‘lib, ochiq ma’lumot butunlay tasodifiy bo‘lsa, $K \geq M$ tengsizlikka ega bo‘linadi. Bu munosabat esa kalitning hajmi (uzunligi) ochiq ma’lumot hajmidan kam bo‘lmasligi kerakligini ko‘rsatadi [10].

Ma’lumotlarni himoya qilishda kriptografiyaga qo‘yiladigan talablar ma’lumotlarning maxfiyligini, yaxlitligini, autentifikatsiyasini va mavjudligini ta’minlashni o‘z ichiga oladi. Ma’lumotlarning maxfiyligini ta’minlash va ma’lumotlarga ruxsatsiz kirishning oldini olish uchun bardoshli shifrlash algoritmlaridan foydalanish kerak. Ma’lumotlarning yaxlitligini ta’minlash va

ma’lumotlar uzatish yoki saqlash vaqtida o‘zgartirilmaganligini ta’minlash uchun autentifikatsiya usullaridan foydalanish talab qilinadi. Autentifikatsiyani ta’minlash uchun faqat avtorizatsiya qilingan foydalanuvchilarning ma’lumotlarga kirishini ta’minlash zarur bo‘ladi. Va nihoyat, ma’lumotlar mavjudligini ta’minlash va ma’lumotlarni yo‘qotishning oldini olish uchun bardoshli kalitlarni boshqarish usullaridan foydalanishni maqsadga muvofiq hisoblanadi.

Shifrlash algoritmlarining kriptobardoshlilik darajasi ishonchliligiga ko‘ra bardoshli bo‘lishi zaruriylik kriteriyi umumiy xususiyatlari tahlil etilib, ularning quyidagicha ekanligi aniqlandi va tasniflari yoritildi.

Tasdiq. *Shifrlash algoritmi mutlaqo bardoshli bo‘lishi uchun, ushbu shartlar bajarilishi zarur:*

1) *o‘rniga qo‘yish shifrlash algoritmlarining ko‘p alifboli sinfga tegishli bo‘lgan ushbu shifrlash jarayoni bosqichlarida ochiq ma’lumot alifbosi belgilarini shifrma’lumot alifbosi belgilariga almashtirish jadvalida shifrma’lumot alifbosi belgilarining joylashish tartibi o‘zgarib turishi kerak;*

2) *kalit uzunligi yetarli katta yoki shifrlash alfaviti belgilari to‘plamining quvvati yetarli katta bu̧lishi lozim*;

3) *aksariyat hollarda algoritmning akslantirish amallari kalitni ifodalovchi alifboning bitta belgisi bilan shifrlanishi kerak bo‘lgan ochiq ma’lumot alifboning ham faqat bitta belgisi ustida bajarilishi kerak;*

4) *x - ochiq ma’lumot alifbo belgilari va y – shifrma’lumot alifbo belgilari ─ shifrqiymatlari statistik bog‘liq emas, ya’ni ixtiyoriy x ochiq ma’lumot va y shifrma’lumot uchun ularning ehtimolligi munosabatlari bilan aniqlanuvchi ushbu tenglik P(X=x/Y=y)=P(X=x) o‘rinli bo‘lishi kerak;*

5) *kalitning hajmi (uzunligi) K ochiq ma’lumot hajmi* (*uzunligi*) *M dan kam bo‘lmasligi lozim: K ≥ M ;*

6) *shifrlash kaliti faqat bir marta ishlatilishi kerak.*

XULOSA

Demak, yuqoridagi fikr-mulohasa va natijalardan, axborot tizimini himoya qilishning zamonaviy kriptografik usullariga qo‘yiladigan umumiy talablar quyidagilardan iborat ekanligi kelib chiqadi:

1. Maxfiylik: shifrlangan ma’lumotlarning asl nusxasini faqat shifrni ochish kaliti ma’lum bo‘lganda tiklash mumkin.

2. Kalitni aniqlash: shifrlash kalitini shifrlangan matnning ma’lum bir qismiga yoki mos keladigan ochiq qismga asoslangan holda aniqlashni hisoblash imkonsiz bo‘lishi kerak.

3. Algoritm tolerantligi: shifrlash algoritmini bilish uning xavfsizligini zaiflashtirmasligi kerak.

4. Kalit sezgirligi: Kalitdagi ozgina o‘zgarish ham shifrlangan ma’lumotlarning sezilarli o‘zgarishiga olib kelishi kerak.

5. Algoritm immuniteti: shifrlash algoritmi elementlari o‘zgarmas bo‘lishi va o‘zgartirilmasligi kerak.

6. Samarali foydalanish: shifrlash jarayonida kiritilgan qo‘shimcha bitlar shifrlangan matnda to‘liq va ishonchli ishlatilishi kerak.

7. Kalit mustaqilligi: shifrlash jarayonida foydalaniladigan kalitlar o‘rtasida

osongina o‘rnatiladigan bog‘liqliklar bo‘lmasligi kerak.

8. Kuchli himoya: Kalitlar to‘plamidan tanlangan shifrlash kaliti ma’lumotlarning ishonchli himoyasini ta’minlashi kerak.

9. Amaliy qo‘llanilishi: Kriptografik algoritm dasturiy ta’minot va texnik nuqtai nazardan amaliy amalga oshirish uchun qulay bo‘lishi kerak. Bundan tashqari, kalit uzunligini o‘zgartirish shifrlash algoritmining sifatini buzmasligi kerak.

Ushbu talablar axborot tizimlarini himoya qilishda kriptografik usullarning xavfsizligi, yaxlitligi va ulardan foydalanish qulayligini ta’minlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. Зенков А. Информационная безопасность и защита информации 2-е изд., пер. и доп. Учебное пособие для вузов. – Litres, 2023.
2. Шнайер Б. Прикладная криптография (Applied Cryptography), 2-е издание //Протоколы, алгоритмы, исходные тексты на языке Си.–610 с. – 2016.
3. Stalling W. Cryptography and network security //Principles and Practices. – 2003.
4. Katz J., Lindell Y. Introduction to modern cryptography: principles and protocols. – Chapman and hall/CRC, 2007.
5. Stinson D. R. Cryptography: theory and practice. – Chapman and Hall/CRC, 2005.
6. Калиновский С. М. Классификация криптографических систем по стойкости. – 2023.
7. Шеннон К. Работы по теории информации и кибернетике. – Рипол Классик, 1963.
8. Хайхан Т. Ю., Никулин В. В. Криптографическая защита информации //Вестник образовательного консорциума Среднерусский университет. Информационные технологии. – 2021. – №. 1. – С. 4-7.
9. Umarov S. A., Akbarov D. E. Working out the new algorithm enciphered the data with a symmetric key //Journal of Siberian Federal University. Engineering & Technologies. – 2016. – Т. 9. – №. 2. – С. 214.
10. Акбаров, Д. Е., Кушматов, О. Э., Умаров, Ш. А., & Орипов, А. (2021). Исследования вопросов критериев криптостойкости алгоритмов непрерывного шифрования. Central asian journal of mathematical theory and computer sciences, 2(11), 25-35.

MUALLIF:
Umarov Shuxratjon Azizjonovich
Fizika-matematika fanlari bo‘yicha falsafa doktori (PhD)

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali “Axborot xavfsizligi” kafedrasi dotsenti

Manzil: Farg‘ona viloyati, Farg‘ona shahri, Mustaqillik ko‘chasi, 185-uy.
Tel.: 732268209, Fax: 732268209

Bog‘lanish uchun: Tel.: +998913961130
E-mail: sh.umarov81@mail.ru

MA’LUMOTLARNI HIMOYALASHDA KRIPTOTIZIMLARNING BARDOSHLI BO‘LISHILIGINI ZARURIYLIK KRITERIYSI

Ushbu maqolada axborotlarni himoya qilishda mumkin bo‘lgan tahdidlar, ma’lumotlar himoyalarini buzish sabablari, tashkilotlardagi axborot xavfsizligiga mas’ul shaxslarning vazifalari bayon qilingan. Shuningdek, axborot tizimini buzuvchining maqsadi tizimdagi zaifliklardan foydalanish va ma’lumotlarga ruxsatsiz kirish yoki tizimni o‘z manfaati uchun manipulyatsiya qilish usullari hamda zamonaviy kriptografik usullariga qo‘yiladigan umumiy talablar va keltirilgan. Ushbu talablar asosida kriptotizmlarning bardoshli bo‘lishiligini zaruriylik kriteriysi bayon qilingan.

Tayanch so‘zlar: kiberhujum, kriptotizim, autentifikatsiya, randomizator, algoritm immuniteti, kalitlarni boshqarish, kriptogramma.

КРИТЕРИЙ НЕОБХОДИМОСТИ СТОЙКОСТИ КРИПТОСИСТЕМ В ЗАЩИТЕ ИНФОРМАЦИИ

В данной статье описаны возможные угрозы защите информации, причины нарушений защиты информации и обязанности лиц, ответственных за информационную безопасность в организациях. Также целью злоумышленника информационной системы является использование слабых мест системы и получение несанкционированного доступа к информации или манипулирование системой в корыстных целях, а также общие требования к современным криптографическим методам. На основе этих требований сформулирован критерий необходимости стойкости криптотизмов.

Ключевые слова: кибератака, криптосистема, аутентификация, рандомизатор, устойчивость алгоритма, управление ключами, криптограмма.

CRITERION FOR THE NEED FOR THE STRENGTH OF CRYPTOSYSTEMS IN INFORMATION PROTECTION

This article describes possible threats to information security, causes of information security violations, and the responsibilities of those responsible for information security in organizations. Also, the goal of an information system attacker is to exploit the weaknesses of the system and gain unauthorized access to information or manipulate the system for personal gain, as well as general requirements for modern cryptographic methods. Based on these requirements, a criterion for the need for the strength of cryptotisms is formulated.

Keywords: cyberattack, cryptosystem, authentication, randomizer, algorithm stability, key management, cryptogram.