TASODIFIY RAQAMLAR GENERATORLARI SIFATINI BAHOLASH MEZONLARI

Akmal Shukurov
Qarshi muhandislik iqtisodiyot instituti “Axborot texnologiyalari” kafedrasi dotsenti, p.f.f.d. (PhD), dotsent.
E-mail: specialist0202@mail.ru
Tel: 93 693-40-04,
Dilfuza Jo‘rayeva
Axborot texnologiyalari va menejment universiteti magistranti,
Tel. 93 908-01-01

Annotatsiya. *Axborot xavfsizligi tizimining vositalarida tasodifiy ketma-ketlik generatorlaridan va tezkor ishlovchi apparat-dasturiy vositalardan foydalanish uchun psevdotasodifiy sonlar ketma-ketligi generatorlarini keng o‘rganish, uzluksiz shifrlash algoritmlarining kriptobardoshlik talablari, gamma ishlab chiqish xususiyatlari va samaradorligi chuqur tahlil qilinishi va yetarli darajada o‘rganilishi kerak.*

Kalit so‘zlar*: Axborot, xavfsizlik, tizim, vosita, generator, algoritm, kriptobardoshlik, talab, ishlab chiqarish, samara, apparat, dastur, loyiha, sanoat.*

Abstract. *For the use of random sequence generators and fast-running hardware-software tools in information security system tools, extensive study of pseudo-random number sequence generators, cryptobardiness requirements of continuous encryption algorithms, gamma development features and efficiency must be thoroughly analyzed and adequately studied.*

Key words: *Information, security, system, tool, generator, algorithm, cryptobark, demand, production, efficiency, hardware, application, project, industry.*

Абстрактный. *Для использования генераторов случайных последовательностей и быстродействующих аппаратно-программных средств в средствах системы информационной безопасности должны быть тщательно проанализированы и адекватно изучены обширные исследования генераторов последовательностей псевдослучайных чисел, требования криптостойкости алгоритмов непрерывного шифрования, особенности и эффективность гамма-разработки.*

Ключевые слова: *Информация, безопасность, система, двигатель, генератор, алгоритм, криптостойкость, спрос, производство, эффект, оборудование, приложение, проект, промышленность.*

Kirish (Introduction). Axborot texnologiyalarini intensiv rivojlanishida axborot xavfsizligi muammolari va ularni yechishning sifati, axborotni himoya qilish tizimlarini yangi turlari va usullarini yaratish ushbu masalalarni dolzarbligini vujudga keltirmoqda. Bu

esa doimiy ravishda tashkilot va korxonalarni himoyalash tizimlaridan to‘g‘ri, samarali, muvaffaqiyatli foydalanishiga bog‘liqdir[1,3].

- Adabiyotlar tahlili (Literature review). Ko‘plab axborotni himoya qilish vositalari tasodifiy raqamlar generatorlari (TRG) asosida qurilmoqda va tashkil etilmoqda. TRG larini qurish muammolari va ularni tadqiq etishda A. Zubkov, A. Sherbakov, D. Knut, B Shnayyer, D.Kelsi, A.Shamir, M. Naor, O. Reyngold, N. Fergyuson, N. A.Kolesova, A.V. Arxangelskaya, I.M.Ajmuxamedov kabi juda ko‘plab olimlar ilmiy tadqiqotlarida ko‘rish mumkin [1,2].

Tadqiqot metodologiyasi (Research Methodology). Tasodifiy raqamlar generatorlari asosida apparat va apparat-dasturiy vositalarni yaratish ustida dunyoning ko‘plab yetakchi ilmiy tadqiqot institutlari va kompaniyalari («Crypto AG» Shveytsariya, «Ankad» Rossiya, «Global Crypto» AQSH, «RSA Data Security» AQSH va boshqa.) tomonidan injenerlik-tadqiqot ishlari olib borilmoqda.

Olib borilgan izlanishlar kriptografik tizimning kriptobardoshligi uning tarkibiga kiruvchi algoritmning mahfiy saqlanishiga bog‘liq bo‘lmay, faqat maxfiy saqlanuvchi kalitgagina bog‘liq qilib yaratish kerakligini keltirib chiqardi va isbotladi. Nisbatan kichik uzunlikka ega bo‘lgan, ya’ni kafolatlangan kriptobardoshlikni ta’minlovchi uzunlikka ega kalit bilan bir tomonlama kriptografik akslantirishlar asosida, yetarli darajada katta uzunlikdagi psevdotasodifiy sonlar ketma-ketligi gammasini ishlab chiqaruvchi generatorlar negizida tezkor uzluksiz shifrlash algoritmlari, bardoshli kalit va boshqa tasodifiy parametrlar ishlab chiqish algoritmlari yaratildi.[2]

Axborot xavfsizligiga taxdidlar va ularni kelib chiqish asoslari, axborotni himoyalashning kriptografik usullari, indentifikatsiya va autentifikatsiya, tasodifiy raqamlar generatorlari va ularning turlari, psevdotasodifiy ketma-ket raqamli generetorlarni tuzilishi va xususiyatlari va boshqa shu kabi maqolaning asosiy qismlarini yortishda foydalanildi.

Tasodifiy raqamlar generatorlari sifatini baxolash mezonlari, yuqori tezlikdagi kvantli tasodifiy raqamlar generatorlari va axborotlarni himoya qilish, tasodifiy raqamlar generatorlarini axborot tizim va kriptografik ilovalarda qo‘llash maqolani yortishda asos sifatida qo‘llanildi.

Internet resurslaridan axborotlarni himoyalash muammolari bo‘yicha C++, Python dasturlash tillarida va 1S8.2 dasturiy platformasida yaratilgan tasodifiy raqamlar generatorini sifatini tadqiq etish va yaratish jarayonida foydalanildi[3, 4].

Axborot xavfsizligiga taxdidlar va ularni kelib chiqish asoslari.

Xavfsizlik – har kuni biz to‘qnashadigan hayotimizning bir muhim ko‘rinishdir. Uyimizning eshigini qulf bilan berkitish, xamyonni saqlash va boshqacha shu kabi turli xavsizlik choralarini ko‘ramiz. Bunday choralarni ham “raqamli dunyoda”, ya’ni kompyuterlar dunyosida ko‘rmaslik mumkin emas.

Umuman olganda axborotni muhofaza qilishning maqsadini quyidagicha ifodalash mumkin:

– axborotni tarqab ketishi, o‘g‘irlanishi, buzilishi, qalbakilash-tirilishini oldini olish;

– shaxs, jamiyat, davlatning xavfsizligiga tahdidni oldini olish;

– axborotni yo‘q qilish, modifikatsiyalash, buzish, nusxa olish, blokirovka qilish kabi noqonuniy harakatlarning oldini olish;

– axborot resurslari va axborot tizimlariga noqonuniy ta’sir qilishning boshqa shakllarini oldini olish, hujjatlashtirilgan axborotga shaxsiy mulk obyekti sifatida huquqiy rejimni ta’minlash;

– axborot tizimida mavjud bo‘lgan shaxsiy ma’lumotlarning maxfiyligini va konfedensialligini saqlash orqali fuqarolarning konstitutsiyaviy huquqlarini himoyalash;

– davlat sirlarini saqlash, qonunchilikka asosan hujjatlashtirilgan axborotlar konfedensialligini ta’minlash;

– axborot jarayonlarida hamda axborot tizimlari, texnologiyalari va ularni ta’minlash vositalarini loyihalash, ishlab chiqish va qo‘llashda subyektlarning huquqlarini ta’minlash.

Axborotni muhofaza qilishning samaradorligi uning o‘z vaqtidaligi, faolligi, uzluksizligi va kompleksligi bilan belgilanadi. Himoya tadbirlarini kompleks tarzda o‘tkazish axborotni tarqab ketishi mumkin bo‘lgan xavfli kanallarni yo‘q qilishni ta’minlaydi. Ma’lumki, birgina ochiq qolgan axborotni tarqab ketish kanali butun himoya tizimining samaradorligini keskin kamaytirib yuboradi.

Axborotni muhofaza qilish sohasidagi ishlar holatining tahlili shuni ko‘rsatadiki, muhofaza qilishning to‘liq shakllangan konsepsiyasi va tuzilishi hosil qilingan, uning asosini quyidagilar tashkil etadi:

- sanoat asosida ishlab chiqilgan, axborotni muhofaza qilishning o‘ta takomillashgan texnik vositalari;
- axborotni muhofaza qilish masalalarini hal etishga ixtisoslash-tirilgan tashkilotlarning mavjudligi;
- ushbu muammoga oid yetarlicha aniq ifodalangan qarashlar tizimi;
- yetarlicha amaliy tajriba va boshqalar.

Biroq, xorijiy matbuot xabarlariga ko‘ra ma’lumotlarga nisbatan jinoiy harakatlar kamayib borayotgani yo‘q, aksincha barqaror o‘sish tendensiyasiga ega bo‘lib bormoqda.

Umumiy yo‘nalishga ko‘ra axborot xavfsizligiga tahdidlar quyidagilarga bo‘linadi:

O‘zbekistonning ma’naviy ravnaqi sohalarida, ma’naviy hayot va axborot faoliyatida fuqarolarning konstitutsiyaviy huquqlari va erkinliklariga tahdidlar;

mamlakatning axborotlashtirish, telekommunikatsiya va aloqa vositalari industriyasini rivojlanishiga, ichki bozor talablarini qondirishga, uning mahsulotlarini jahon bozoriga chiqishiga, shuningdek mahalliy axborot resurslarini yig‘ish, saqlash va samarali foydalanishni ta’minlashga nisbatan tahdidlar;

Respublika hududida joriy etilgan hamda yaratilayotgan axborot va telekommunikatsiya tizimlarining meyorida ishlashiga, axborot resurslari xavfsizligiga tahdidlar.

Umuman olganda kompyuter muxiti ikki xil xavf-xatarga duchor bo‘lishi mumkin:

1. Ma’lumotlarni yo‘qolishi yoki o‘zgartirilishi.

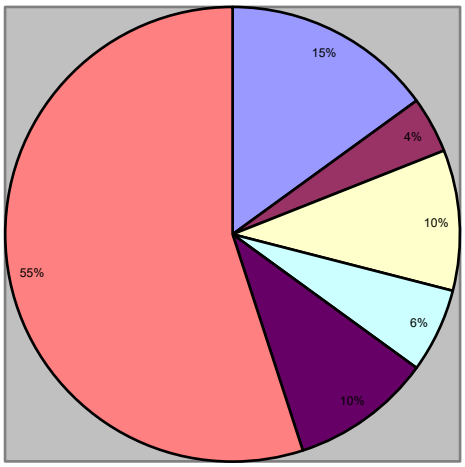
2. Servisning to‘xtalishi.

Bunda inson xatoliklari xavfsizlikki jiddiy taxdid tug‘diradi va xavfsizlikni buzilish manbalarini oldini olish choralarini ko‘rishni talab qiladi. Xavfsizlikni buzilish manbalariga quyidagilarni kiritish mumkin (1-rasmga qarang):

– Fizik xavsizlik muammolari;
– Viruslar;
– Vijdonsiz xodimlar;
– Xafa bo‘lgan xodimlar;
– Tashqaridan bo‘ladigan atakalar;
– Foydalanuvchi va xodimlar xatoliklari.

Statistik ma’lumotlarga ko‘ra bu xolatni quyidagi diagrammada to‘liq taxlil qilish mumkin:

Xavsizlikni buzilish manblari



1-rasm. Xavfsizlikni buzilish manbalari.

Axborot hisoblash tizimlarida axborot xavfsizligini ta’minlash nuqtai nazaridan o‘zaro bog‘liq bo‘lgan uchta tashkil etuvchini ko‘rib chiqish maqsadga muvofiq:

1. Axborot;
2. Texnik va dasturiy vositalar;
3. Xizmat ko‘rsatuvchi personal va foydalanuvchilar.

Tahdidning uchta ko‘rinishi mavjud.

1. Konfedensiallikning buzilishiga tahdid shuni anglatadiki, bunda axborot unga ruxsati bo‘lmaganlarga ma’lum bo‘ladi. Bu holat konfedensial axborot saqlanuvchi tizimga yoki bir tizimdan ikkinchisiga uzatilayotganda noqonuniy foydalana olishlikni qo‘lga kiritish orqali yuzaga keladi.

2. Butunlikni buzishga tahdid hisoblash tizimida yoki bir tizimdan ikkinchisiga uzatilayotganda axborotni har qanday qasddan o‘zgartirishni o‘zida mujassamlaydi. Jinoyatchilar axborotni qasddan o‘zgartirganda, bu axborot butunligi buzilganligini bildiradi. Shuningdek, dastur va apparat vositalarning tasodifiy xatosi tufayli axborotga

noqonuniy o‘zgarishlar kiritilganda ham axborot butunligi buzilgan hisoblanadi. Axborot butunligi axborotning buzilmagan holatda mavjudligidir.

3. Xizmatlarning izdan chiqish tahdidi hisoblash tizimi resurslarida boshqa foydalanuvchilar yoki jinoyatchilar tomonidan ataylab qilingan harakatlar natijasida foydalana olishlilikni blokirovka bo‘lib qolishi natijasida yuzaga keladi. Axborotdan foydalana olishlilik – axborot aylanuvchi, subyektlarga ularni qiziqtiruvchi axborotlarga o‘z vaqtida qarshiliklarsiz kirishini ta’minlab beruvchi hamda ixtiyoriy vaqtda murojaat etilganda subyektlarning so‘rovlariga javob beruvchi avtomatlashtirilgan xizmatlarga tayyor bo‘lgan tizimning xususiyatidir.[2]

Natijalar va muhokama (Result and Discussions). Identifikatsiya va autentifikatsiyaning mohiyatini ochishga keng to‘htalib, autentifikatsiyaning asosiy ko‘rinishlari hamda foydalanuvchi va jarayonlar to‘g‘risidagi ma’lumotlarning haqiqiyligini (aslligini) tekshirish va aniqlash jarayonlarini o‘rganilgan[1].

- Xulosa va takliflar (Conclusion/Recommendations) O‘zbekistonning ma’naviy ravnaqi sohalarida, ma’naviy hayot va axborot faoliyatida fuqarolarning konstitutsiyaviy huquqlari va erkinliklariga tahdidlarni interent tarmog‘i hamda axborotni qayta ishlash vositalaridagi axamiyatini respublika hududida joriy etilgan hamda yaratilayotgan axborot va telekommunikatsiya tizimlarining meyorida ishlashiga, axborot resurslari xavfsizligini ta’minlashga bog‘liqligi xususida fikrlar berilgan[3].

ADABIYOTLAR:

1. Шнайер Б. Прикладная криптография: протоколы, алгоритмы и исходные тексты на языке С, часть 3. - М.: Триумф, 2002. - 816 с.
2. Иванов, М.А. Криптографические методы защиты информации / М.А. Иванов.- М.: КУДИЦ-ОБРАЗ, 2001.-368с. (Илмий мақола ва тадқиқот)
3. Варфоломеев, А.А. Управление ключами в системах криптографической защиты банковской информации / А.А. Варфоломеев, О.С. Домина, М.Б. Пеленицын.- М.: МИФИ, 1996.- 128 с. (Илмий мақола ва тадқиқот)
4. Шифрование — асимметричные методы. Глава 8 ("Шифрование с открытым ключом", "Обмен ключом без обмена ключем", "Криптографическая стойкость", "Задача Диффи-Хеллмана и задача дискретного логарифмирования")
5. I.Tojimamatov, D.Xalilov, “Tasodifiy raqamlar generatorlari sifatini baxolash mezonlari” (Toshkent, 13-14-mart 2014 y.) 173, 174, 175 bet.
6. I.Tojimamatov, D.Xalilov, “Yuqori tezlikdagi kvantli tasodifiy raqamlar generatorlari va axborotlarni himoya qilish”, ilmiy-amaliy konferensiya (Farg‘ona, 2014 y.). 110-112 bet.
7. I.Tojimamatov, D.Xalilov, “Tasodifiy raqamlar generatorlarini axborot tizimi va kriptografik ilovlarda qo‘llash”, xalqaro ilmiy-texnik konferensiya (Andijon, 2014 y.) 148-151 bet.

8. Shukurov A.U., “Bulutli texnologiyalari asosida talabalarning virtual texnologiyalardan foydalanish kompetentligini rivojlantirish metodikasini takomillashtirish (Axborot texnologiyalari fani misolida)”. Pedagogika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi avtoreferati. Qarshi. 2023.-52 b.

9. Akmal Shukurov, “Texnika ixtisosliklari ta’limida axborotlarni loyihalashtirishda axborot texnologiyalari fanini o‘qitishning zamonaviy metodlari”. “Ta’lim, fan va innovatsiya”. ma’naviy-ma’rifiy, ilmiy-uslubiy jurnal (2024 yil № 1). 116-119-b.

10. Shukurov Akmal Uktamovich, “ Basic professional rules for students of a higher educational institution in the design of information”. International Conference on Research in Humanities, Applied Sciences and Education. Germany. February 27 th 2024. 8-14 p.

11. Shukurov A. U, “Texnika ixtisosliklari otmida loyihali-axborot ta’lim tizimni shakllantirish”. “Ta’limda zamonavty axborot-kommunikatsiya texnologiyalarini qo‘llash afzalliklari, muammolari va yechimlari”. Respublika ilmiy-amaliy konferensiya 2024. 81-86 b.