

Dilmurod Solijonovich TUXTANAZAROV

*O'zbekiston xalqaro islom akademiyasi
"Zamonaviy axborot-kommunikatsiya
texnologiyalari" kafedrası PhD*

Sardorbek Obobakirjon o'g'li BUVASHEV

*O'zbekiston xalqaro islom akademiyasi
"Zamonaviy axborot-kommunikatsiya
texnologiyalari" kafedrası magistranti*

KIBERMAKONDA XAVFSIZLIKNI TA'MINLASHNING ZAMONAVIY USUL VA ALGORITMLARI

СОВРЕМЕННЫЕ МЕТОДЫ И АЛГОРИТМЫ КИБЕРБЕЗОПАСНОСТИ

MODERN CYBER SECURITY METHODS AND ALGORITHMS

Ushbu maqolada kiber jinoyat turlari va ularga qarshi olib borilayotgan choralar keltirilgan. Kiber xavfsizlik masalalarining dolzarbligi va ularning statistik tahlillari keltirilgan. Bu borada O'zbekistonda olib borilayotgan ishlar tahlili keltirilgan. Dunyo bo'yicha ko'p ishlatilgan parollar statistikasi va parollarni generatsiya qilish usullari keltirilgan.

Kalit so'zlar: *Axborot xavfsizligi, kibermakon, parollar, kontsepsiya, dasturiy vositalar, kiberxavfsizlik, kiberhujumlar.*

В этой статье описаны виды киберпреступлений и меры, принимаемые против них. Представлена актуальность вопросов кибербезопасности и их статистический анализ. Анализируется работа, проводимая в Узбекистане в этом направлении. Вот статистика наиболее часто используемых паролей в мире и способов их генерации.

Ключевые слова: *информационная безопасность, киберпространство, пароли, концепция, программное обеспечение, кибербезопасность, кибератаки.*

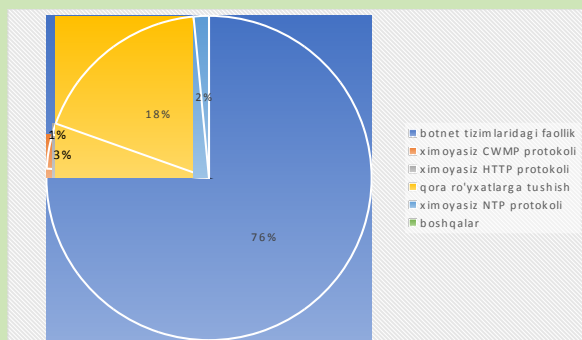
This article describes the types of cybercrime and the measures taken against them. The relevance of cybersecurity issues and their statistical analysis are presented. The work carried out in Uzbekistan in this direction is analyzed. Here are the statistics of the most used passwords in the world and how they are generated.

Keywords: *information security, cyberspace, passwords, concept, software, cybersecurity, cyber attacks.*

Kirish. Hozirgi paytda rivojlangan davlatlarda innovatsion jarayonlarni rivojlantirish asosan global tarmoqlar asosida amalga oshirilmoqda hamda innovatsion infrastrukturalar tashkil etilmoqda. Bularning barchasi bir tomondan raqamli iqtisodiyotga o'tayotganligi, ishlab chiqarish samaradorlik darajasini oshishiga va umuman hayot sifatini yaxshilanishiga mo'ljallangan bo'lsa, ikkinchi tomondan axborotlashtirish jarayonida yangi xavf va xatarlarni kelib chiqishiga sabab bo'lmoqda. Hozirda internet har kunlik hayotning eng tez o'sayotgan infratuzilmasidir. Shu sababli eng so'nggi texnologiyalar inson yashash tarzini o'zgartirib bormoqda va axborotlarimizni eng samarali yo'l bilan ham xavfsiz saqlash dolzarb muammoga aylandib kelmoqda hamda shular bilan bir qatorda kiber jinoyatlar kundan-kunga ko'payib jiddiy xavfga aylanib bormoqda. Yani bugungi kunda inson shunchaki bitta tugmani bosish, e-mail, audio yoki video orqali har qanday ma'lumotni tarmoqda uzatish va qabul qilish imkoniyatiga ega, lekin u ma'lumotni qay darajada xavfsiz almashilayotganligi yoki boshqa insonga axborot qanchalik xavfsiz yetib borayotganligi xar bir rivojlangan davlatlar uchun muhim vazifa sifatida qaralmoqda. Jumladan O'zbekistonda ham kiber xavfsizlik bo'yicha bir qancha muammolar mavjud. Rivojlangan davlatlarda 60% dan ortiq moliyaviy kelishuvlar internet orqali amalga oshiriladi, shuning uchun bu soha katta miqdordagi kelishuvlar uchun eng yaxshi sifatli xavfsizlikni talab qiladi. Kiber xavfsizlikning ko'lami faqatgina axborot texnologiyalari sanoatida axborotni himoyalash emas, balki kibermakon kabi boshqa ko'pgina turlarga bo'linadi.

Kiberxavfsizlik deganda, shaxsiy ma'lumotlarni o'g'irlash va tarmoqlar, dasturlar, qurilmalar, shikastlanishlar va ruxsatsiz kirishdan himoya qilish yani onlayn ravishda qilingan barcha hujum amaliyotlari uchun qilingan xavfsizlik choralari tushuniladi. U maxfiy ma'lumotlarga kirish, o'zgartirish yoki yo'q qilish kabi kiberhujumlardan himoya qiladi [1]. Hozirgi kunda barcha axborot tizimlari uchun maxfiylik auditini o'tkazadigan, so'nggi tahdidlarni topadigan va ularni bartaraf etadigan ko'plab kiberxavfsizlik vositalari mavjud ammo ular ham yetarli darajada xavfsizlikni

ta'minlay olmaydi. 1903 yilda birinchi kiber hujum boshlandi va shundan keyin tez-tez jinoyatlar sodir bo'la boshladi. Kiber jinoyatchilikning yangi usullari paydo bo'la boshladi. Tarmoqda ma'lumotlarni o'g'irlanishi, zo'ravonlik va kiber terrorizm hozirgi kunda insonlar va davlatlar uchun katta muammoga aylanib kiber jinoyat ham texnologik rivojlanishlar bilan o'sib bormoqda. Ijtimoiy tarmoqlar bizni oilamiz va do'stlarimiz bilan xafsiz muloqot qila oladigan saytlar bilan ta'minlayotganiga qaysidir manoda ishonamiz. Ammo kiber jinoyatchilar ijtimoiy tarmoqlarda insonlarning shaxsiy ma'lumotlarini o'g'irlash va foydalanishda davom etmoqda[2]. Nafaqat ijtimoiy tarmoqlarda, balki bank kelishuvlarida ham ushbu holatlar kuzatilmoqda. Jumladan O'zbekistonda xam bir qancha kiber tahdidlar amalga oshirilgan, buni "Kiberxavfsizlik markazi" DUK tomonidan tayyorlangan 2020 yil yakuniy hisobotlarida xam ko'rish mumkun.



1-расм.

Monitoring natijalariga ko'ra axborot va kiberxavfsizlikka tahdid soluvchi 27 000 000 dan ortiq zararli tarmoq xodisalari kuzatilgan. Tekshiruv natijalariga ko'ra kiberxujumlar asosan Ruminiya, Germaniya, Misr, Slovakiya, AQSH, Indoneziya, Xitoy, Rossiya Federatsiyasi, Buyuk Biritaniya, Fransiya, Saudiya Arabistoni, Tunis, Ukrainiya, Gollandiya, Janubiy Koreya, Kanada, Turkiya, Polsha, Vetnam, Xindiston mamlakatlariga tegishli internet manzillaridan amalga oshirilgan. 2020 yilda 2019 yilga nisbatan 144% ga yuqorilagani aniqlangan.

Hozirgi kunda foydalanuvchilar internetda har kuni ko'plab yangi tizimlarda ishlash uchun akkauntlar yaratishadi[3,4]. Bu jarayonda foydalanuvchidan eslab qolishga qulay bo'lgan va boshqalar uchun murakkab parol terish talab etiladi.

Masalaning qo'yilishi. F-Secure kompaniyasining kiberxavfsizlik bo'yicha mutaxassislari eng ishonchsiz parollar ro'yxatini e'lon qildi. Bular – pochta yoki biror servisdagi akkaunt paroli emas, balki turli qurilmalarga qo'yilgan parollardir. Parollarni boshqarish yo'nalishidagi NordPass kompaniyasi o'z ma'lumotlar bazasini o'rganib chiqib, foydalanuvchilar haliyam o'ta sodda va buzish oson bo'lgan parollarni qo'llashayotganini aniqladi. Deyarli 275,7 million parolni tekshirib ko'rgan mutaxassislar 2020 yilda onlayn-akkauntlar uchun eng ko'p ishlatilgan parollarni e'lon qilishdi.

Antireytingda birinchi o'rinni «123456» paroli oldi – undan 2,5 million kishi foydalanmoqda. 2019 yilgi reytingda esa u ikkinchi o'rinda edi. NordPass bayonotiga ko'ra, xakerlar va havaskorlar bu parolni 23,5 million martadan oshiq buzishgan. 2019 yilgi reyting «yetakchisi» bo'lgan «12345» parolini 2020 yil ham 188 000 mingdan oshiq foydalanuvchi ishlatgan va u reytingda sakkizinchi o'rindan joy olgan. Yuqoridagi keltirilgan parollarni buzish uchun xakerlarga bir soniyadan ham kamroq vaqt yetarli bo'ladi. 2020 yilgi ro'yxatga kirgan parollarning yarmidan ozrog'i yangi parollar bo'lgan. Shulardan biri – «picture1» paroli yangi bo'lsa-da, birdaniga uchinchi o'rinni zabt etgan. Shunisi ham borki, reyting boshidagi o'ntalikka kirgan ayrim parollarni buzishga bir necha soniya kifoya qilgan bo'lsa, «picture1» uchun xakerlar uch soatcha ter to'kishlariga to'g'ri kelgan. Keyingi pog'onadan ko'pchilik ishlatadigan «password» so'zi joy olgan. Yana bir yangi so'z – «senha» ham kuchli o'ntalikka kirgan. U portugalchada «parol» ma'noni anglatadi.

2-rasm. Ko`p ishlatilgan parollar

Eng yuqori oʻntalikka «11111» paroli ham kirgan – u 17-oʻrindan 6-pogʻonaga koʻtarilib olgan. Oʻtgan yilgi roʻyxatda 18-oʻrinda turgan «123123» ham bu gal yettinchi qatorga chiqqan. Ommabop kombinatsiya – «qwerty» bu yil

12-o'rindan joy olgan.

Tadqiqotlar shuni ko'rsatmoqdaki, qulayligi sababli kishilar oson eslab qolinuvchi va sodda parollarni tanlashmoqda. Shuningdek, parol sifatida nomaqbul so'zlar, sonlar, kishi ismlari va taom nomlarini qo'llash hollari ko'p uchramoqda.

Masalani yechilishi. Bu borada akkauntingizni buzib kirishdan saqlash usullari, ishonchli parol yaratish yo'llari, parolingizni buzish qanchalik osonligini onlayn tekshirish, parolingiz o'g'irlanganini tekshirib beruvchi tizimlar mavjud. Agar biror servis uchun tanlagan parolingiz qanchalik ishonchli ekanligini bilmoqchi bo'lsangiz, «Kasperskiy laboratoriyasi» buni onlayn tarzda tekshirish imkonini taqdim etadi.

Quyidagi havola orqali parolingizni tekshirib olishingiz mumkin: <https://password.kaspersky.com/ru/>

Tekshirmoqchi bo'lgan parolingizni «Test your password» maydonchasiga tering va tekshiruv natijasini ko'ring[4,5].

3-rasm. Kasperskiy laboratoriyasining parolni tekshirish tizimi

Parolni terish maydonchasining pastida, uni buzish uchun oddiy kompyuterda qancha vaqt kerak bo'lishi aks ettiriladi. Agarda bu ko'rsatkich o'n yildan kam bo'lsa, uning o'rniga boshqa – ishonchliroq parol tanlashni maslahat beramiz. Zero, saytda ko'rsatilgani – parolingizni oddiy kompyuterda buzish uchun talab etiluvchi muddatdir; jiddiy qasd qilgan xakerlar esa uni bir necha kun ichida ham buza olishlari mumkin.

Xulosa. Shunday qilib, axborot texnologiyalarining rivoji va axborotlashtirilgan jamiyatning shakllanishi qator ijobiy va salbiy jihatlar kasb etib, ma'lum bir muammolarni keltirib chiqadi. Ushbu vujudga keladigan muammolarning kiber xavfsizligi sohasiga taalluqli bo'lganlari ko'plab bo'lib, bularga axborot xavfsizligini

ta'minlash, axborot quroli va axborot urushlari, kompyuter jinoyatchiligi va uning oldini olish, normativ huquqiy asos yaratish, qat'iy javobgarlik belgilash va xokazolarni kiritishimiz mumkin. Bu vujudga kelayotgan muammolar o'z navbatida chuqur o'rganilib o'z yechimini topmog'i lozim.

FOYDALANILGAN ADABIYOTLAR

1. I.M.Karimov “Axborot xavfsizligi asoslari”. Toshkent-2013, 156 b.
2. Крат Ю.Г., Шрамкова И.Г. Основы информационной безопасности: учеб. пособие - Хабаровск: Изд-во ДВГУПС, 2008. - С 75.
3. Мельников В.Н., Клейменов С.А. Информационная безопасность и защиты информации. Москва 2008.
4. <https://www.terabayt.uz/>
5. <https://www.f-secure.com/en>