PAROL XAVFSIZLIGI: KUCHLI PAROL YARATISH, PAROL MENEJERLARI VA HISOB O‘G‘IRLANISHI HOLATLARI

Samarqand iqtisodiyot va servis instituti

"XALQARO IQTISODIY MUNOSABATLAR" fakulteti

Iqtisodiy xavfsizlik yo‘nalishi

IKX-123 4-KURS

Islomova Sevaraxon Olimovna

+998930890085

islomovasevaraxon@gmail.com

Samarqand iqtisodiyot va servis instituti

Axborot texnologiyalari kafedrasi asistenti

Rustamov Sherzod Norxudjayevich

Annotatsiya:

Mazkur maqolada raqamli xizmatlar keng joriy etilayotgan sharoitda parol xavfsizligining nazariy-huquqiy asoslari, kuchli parol yaratish mezonlari, parol menejerlarining samaradorligi hamda hisoblarning o‘g‘irlanishi (account takeover) holatlari mexanizmlari kompleks tahlil qilinadi, parol xavfsizligining konstitutsiyaviy-huquqiy kafolatlar bilan aloqasi ochib beriladi. Tadqiqotning maqsadi — O‘zbekiston Respublikasi normativ-huquqiy bazasi va xalqaro ilmiy tajriba asosida foydalanuvchi autentifikatsiyasi xavfsizligini oshirishning ilmiy asoslangan yondashuvlarini asoslashdan iborat. Mavzuning dolzarbligi “Raqamli O‘zbekiston — 2030” strategiyasi doirasida davlat va tijorat xizmatlarining onlayn shaklga o‘tishi, shaxsga doir ma’lumotlar hajmining ortishi hamda ma’lumotlar sizib chiqishi natijasida ochiqqa chiqqan parollardan foydalanuvchi hujumlarning kengayishi bilan belgilanadi. Tadqiqotda qiyosiy-huquqiy tahlil, tizimli yondashuv, ilmiy adabiyotlarni tahlil qilish va xalqaro standartlar (NIST SP 800-63B) mazmunini taqqoslash usullaridan foydalanildi. Natijalar shuni ko‘rsatdiki, parol

xavfsizligi uzunlik, noyoblik va oldindan taxmin qilib bo‘lmaslik mezonlariga tayanishi lozim; majburiy davriy almashtirish va murakkab belgilarga qo‘yiladigan rasmiy talablarning samarasi cheklangan; parol menejerlari va ko‘p faktorli autentifikatsiya esa hisob o‘g‘irlanishi xavfini sezilarli kamaytiradi. Maqola oxirida normativ-huquqiy, tashkiliy va amaliy takliflar hamda foydalanuvchilar va operatorlar uchun tavsiyalar shakllantirildi.

Kalit so‘zlar: parol xavfsizligi, kuchli parol, autentifikatsiya, parol menejeri, hisob o‘g‘irlanishi, kiberxavfsizlik, ma’lumotlar sizib chiqishi, ko‘p faktorli autentifikatsiya, shaxsga doir ma’lumotlar, kredensiallarni to‘ldirish hujumi.

Abstract:

The article provides a comprehensive analysis of the theoretical and legal foundations of password security, the criteria for creating strong passwords, the effectiveness of password managers, and the mechanisms of account takeover in the context of the widespread digitalization of public and commercial services. The aim of the study is to substantiate scientifically grounded approaches to improving the security of user authentication on the basis of the regulatory framework of the Republic of Uzbekistan and international research experience. The relevance of the topic is determined by the transition of government and commercial services online within the “Digital Uzbekistan — 2030” strategy, the growing volume of personal data, and the expansion of attacks that exploit credentials exposed in data breaches. Comparative legal analysis, a systemic approach, a review of scientific literature, and a comparison of international standards (NIST SP 800-63B) were used as research methods. The results demonstrate that password security should rely on the criteria of length, uniqueness, and unpredictability; that mandatory periodic changes and formal complexity requirements have limited effectiveness; and that password managers and multi-factor authentication substantially reduce the risk of account takeover. Normative-legal, organizational, and practical proposals, as well as recommendations for users and operators, are formulated at the end of the article.

Keywords: password security, strong password, authentication, password manager, account takeover, cybersecurity, data breach, multi-factor authentication, personal data protection, credential stuffing.

KIRISH

XXI asrda raqamli texnologiyalar iqtisodiyot, ta’lim, sog‘liqni saqlash, davlat boshqaruvi va shaxslararo muloqotning ajralmas infratuzilmasiga aylandi. Elektron pochta, ijtimoiy tarmoqlar, mobil bank ilovalari, davlat xizmatlari portallari kabi onlayn xizmatlarning aksariyatida foydalanuvchi shaxsini tasdiqlashning asosiy va eng keng tarqalgan vositasi parol bo‘lib qolmoqda. Aslida parol raqamli muhitdagi shaxsning “kaliti” vazifasini bajaradi: unga ega bo‘lgan shaxs hisob egasining nomidan xabar yuborishi, mablag‘larni ko‘chirishi, maxfiy hujjatlarni o‘qishi va boshqa xizmatlardagi hisoblarni tiklash jarayonlarini boshqarishi mumkin. Parollarni saqlash va himoya qilish muammosi ilmiy jihatdan yarim asrdan ko‘proq vaqt avval, 1979-yilda R. Morris va K. Tompson tomonidan tizimli o‘rganilgan bo‘lsa-da,[1] bugungi kunda ham o‘z dolzarbligini yo‘qotmadi; aksincha, foydalanuvchi boshqaradigan hisoblar sonining ko‘payishi va ularga qaratilgan hujumlarning murakkablashishi bilan yanada keskinlashdi.

Mavzuning huquqiy dolzarbligi, avvalo, konstitutsiyaviy normalar bilan belgilanadi. 2023-yil 30-aprelda umumxalq referendumida qabul qilingan O‘zbekiston Respublikasi Konstitutsiyasining yangi tahririda har kimning shaxsiy hayotining daxlsizligiga, shaxsiy va oilaviy sirga ega bo‘lish huquqi hamda shaxsga doir ma’lumotlarini himoya qilish kafolati mustahkamlangan.[2] Biroq konstitutsiyaviy huquqning amalda ta’minlanishi uchun faqat deklarativ normalarning o‘zi yetarli emas: fuqaroning elektron pochtasi, bank hisobi yoki davlat xizmatlaridagi profili ruxsatsiz egallab olinsa, bu huquq real ravishda buziladi. Shu ma’noda, ishonchli autentifikatsiya vositalari, jumladan, to‘g‘ri parol amaliyoti

[1]Morris R., Thompson K. Password security: a case history // Communications of the ACM. — 1979. — Vol. 22, No. 11. — P. 594–597.

[2]O‘zbekiston Respublikasi Konstitutsiyasi (2023-yil 30-aprelda umumxalq referendumida qabul qilingan yangi tahriri), 31-modda // Milliy qonunchilik ma’lumotlari bazasi (Lex.uz). URL: https://lex.uz

konstitutsiyaviy kafolatlarning texnik-tashkiliy mexanizmi sifatida namoyon bo‘ladi. Demak, parol xavfsizligi masalasi faqat texnik muammo emas, balki inson huquqlarini himoya qilishning ajralmas tarkibiy qismidir.

Sohani tartibga soluvchi qonunchilik tizimida 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun alohida o‘rin tutadi. Mazkur Qonun shaxsga doir ma’lumotlarni yig‘ish, tizimlashtirish, saqlash va boshqa tarzda qayta ishlash bilan bog‘liq munosabatlarni tartibga solib, ma’lumotlar operatori va egasiga ularni himoya qilish bo‘yicha huquqiy, tashkiliy va texnik choralarni ko‘rish majburiyatini yuklaydi.[3] Foydalanuvchi hisob yozuvlari, login-parol juftliklari va parollarning xesh-qiymatlari ham amalda shaxsni identifikatsiyalash imkonini beruvchi ma’lumotlar tarkibiga kirgani sababli, ularning xavfsiz saqlanishi operator zimmasidagi huquqiy majburiyatning ajralmas qismi hisoblanadi. Qonunning mohiyati shundan iboratki, ma’lumotlar sizib chiqqan taqdirda javobgarlik faqat hujumchiga emas, balki himoya choralarini yetarli darajada ko‘rmagan operatorga nisbatan ham yuzaga kelishi mumkin.

Parollarni majburiy davriy almashtirish amaliyoti ham ilmiy tanqidga uchragan. Y. Chjan, F. Monrouz va M. Rayter parol amal qilish muddatining xavfsizligini empirik tahlil qilib, avvalgi parolni bilgan hujumchi uchun yangi parol ko‘pincha o‘ta oson topilishini, tahlil qilingan hisoblarning katta qismida (taxminan 41 foizida) keyingi parolni oflayn rejimda soniyalar ichida aniqlash mumkin bo‘lganini ko‘rsatgan.[4] AQSh Federal savdo komissiyasining o‘sha paytdagi bosh texnologi L. Kranor ham majburiy almashtirish amaliyotini qayta ko‘rib chiqish zarurligini ochiq asoslagan.[5] Buyuk Britaniyaning Milliy kiberxavfsizlik markazi (NCSC) ham parol siyosatini soddalashtirish, majburiy muddatli

[3]O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni // Milliy qonunchilik ma’lumotlari bazasi (Lex.uz). URL: https://lex.uz

[4]Zhang Y., Monrose F., Reiter M.K. The security of modern password expiration: an algorithmic framework and empirical analysis // Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS ’10). — ACM, 2010. — P. 176–186.

[5]Cranor L. Time to rethink mandatory password changes // Federal Trade Commission, Tech@FTC blog. — 2016, 2-mart. URL: https://www.ftc.gov

almashtirishdan voz kechish va tasodifiy so‘zlardan iborat uzun parollarni targ‘ib qilish yo‘nalishida tavsiyalar ishlab chiqqan.[6] Yevropa Ittifoqining Shaxsga doir ma’lumotlarni himoya qilish umumiy reglamenti (GDPR) 32-moddasi esa ma’lumotlarni qayta ishlash xavfsizligini ta’minlash uchun xavf darajasiga mos texnik va tashkiliy choralarni ko‘rishni talab qiladi, bu esa “yagona qat’iy parol qoidasi” emas, balki xavfga mutanosib yondashuv tamoyilini ifodalaydi.[7]

Kuchli parolning amaliy mezonlarini miqdoriy jihatdan quyidagicha ko‘rsatish mumkin (mualliflik hisob-kitoblari, tasviriy xarakterga ega). 94 ta bosma ASCII belgidan tasodifiy tanlangan sakkiz belgili parol uchun mumkin bo‘lgan variantlar soni 94 sakkizinchi darajada, ya’ni taxminan $6{,}1 \cdot 10^{15}$ (taxminan 52,4 bit) ni tashkil etadi. Agar hujumchi tez xeshlanadigan (masalan, tuzsiz va sekinlashtirilmagan) xeshga ega ma’lumotlar bazasini oflayn rejimda soniyasiga taxminan 10^{10} ta urinish tezligida buzsa, bunday fazoni to‘liq ko‘rib chiqish taxminan yetti sutkani talab qiladi. Tasodifiy tanlangan 12 belgili parol uchun variantlar soni taxminan $4{,}8 \cdot 10^{23}$ (taxminan 78,7 bit) bo‘lib, xuddi shu tezlikda uni to‘liq qidirish bir milliondan ortiq yilni talab qiladi. Xuddi shunday, 7776 so‘zdan iborat ro‘yxatdan tasodifiy tanlangan oltita so‘zdan tuzilgan parol-ibora (Diceware usuli) taxminan 77,5 bit chidamlilikni ta’minlaydi va eslab qolish nuqtai nazaridan ancha qulaydir. Muhim shart shundaki, bu hisob-kitoblar faqat belgilar yoki so‘zlar tasodifiy mexanizm yordamida tanlangan holatda to‘g‘ri bo‘ladi; inson tomonidan o‘ylab topilgan, ko‘rinishdan murakkab parollar yuqorida ko‘rib chiqilgan lug‘at va qoidalarga asoslangan hujumlar tufayli nazariy ko‘rsatkichdan bir necha tartibga kam chidamlilikka ega bo‘ladi.

Parollarni qayta ishlatish — hisob o‘g‘irlanishining asosiy omillaridan biri. A. Das va hamkasblari parollarning qayta ishlatilishi va ozgina o‘zgartirilishi hodisasini o‘rganib, foydalanuvchilarning katta qismi (taxminan 43 foizi) bir xil yoki o‘xshash parollardan turli

[6]National Cyber Security Centre (UK). Password administration for system owners and the NCSC password guidance collection. URL: https://www.ncsc.gov.uk/collection/passwords

[7]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Article 32 // Official Journal of the European Union. — 2016. — L 119. — P. 1–88.

saytlarda foydalanishini, bunday o‘xshashlik esa bitta saytdan sizib chiqqan paroldan boshqa hisoblarga hujum qilishda foydalanilishini ko‘rsatgan.[8] S. Pirman va hamkasblari real foydalanuvchilarning parol xulq-atvorini tabiiy sharoitda kuzatib, parollarning qayta ishlatilishi va ozgina o‘zgartirilishi keng tarqalganini tasdiqlagan.[9] K. Tomas va hamkasblarining Google bilan hamkorlikdagi keng ko‘lamli tadqiqoti milliardlab sizib chiqqan hisob ma’lumotlari va fishing hamda klaviatura josuslari (keylogger) orqali o‘g‘irlangan ma’lumotlarni tahlil qilib, ma’lumotlar sizib chiqishidan olingan parollarning taxminan 7 foizi, fishing orqali olinganlarining esa taxminan 25 foizi qurbonning amaldagi Google paroli bilan mos kelganini aniqlagan.[10] B. Pal va hamkasblari neyron tarmoqlar asosida parol o‘xshashligi modellarini yaratib, hujumchi ma’lum paroldan uning oddiy o‘zgartirilgan variantlarini samarali sinab ko‘rishi mumkinligini ko‘rsatgan, ya’ni “Parol1” ni “Parol2” ga almashtirish himoya bermaydi.[11]

Hisob o‘g‘irlangani gumon qilingan yoki aniqlangan holatda izchil harakat qilish muhim: boshqa qurilmadan parolni darhol yangi, noyob va uzun parolga almashtirish va barcha faol seanslarni tugatish; shu yoki o‘xshash parol ishlatilgan boshqa hisoblar (birinchi navbatda elektron pochta va moliyaviy xizmatlar) parollarini o‘zgartirish; ko‘p faktorli autentifikatsiyani yoqish va tiklash kanallarini tekshirish; moliyaviy zarar xavfi bo‘lsa, bankni xabardor qilish va kartani bloklash; hodisa haqida xizmat ko‘rsatuvchiga, zarur hollarda vakolatli davlat organlari va huquqni muhofaza qilish idoralariga xabar berish; kredensiallar qaysi kanal orqali sizib chiqqanini aniqlash.

[8]Das A., Bonneau J., Caesar M., Borisov N., Wang X. The Tangled Web of Password Reuse // Network and Distributed System Security Symposium (NDSS 2014). — Internet Society, 2014.

[9]Pearman S., Thomas J., Naeini P.E. et al. Let’s Go in for a Closer Look: Observing Passwords in Their Natural Habitat // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. — ACM, 2017.

[10]Thomas K., Li F., Zand A. et al. Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. — ACM, 2017.

[11]Pal B., Daniel T., Chatterjee R., Ristenpart T. Beyond Credential Stuffing: Password Similarity Models Using Neural Networks // 2019 IEEE Symposium on Security and Privacy. — IEEE, 2019.

Yuqoridagi tahlil asosida parol xavfsizligining ko‘p qatlamli (chuqur himoya) modelini taklif etish mumkin. Birinchi qatlam — har bir xizmat uchun noyob va yetarli darajada uzun (kamida 14–16 belgi yoki 5–6 ta tasodifiy so‘zdan iborat) parol-iborasi. Ikkinchi qatlam — parol menejeri yordamida parollarni yaratish va saqlashni avtomatlashtirish. Uchinchi qatlam — ko‘p faktorli yoki fishingga chidamli autentifikatsiya. To‘rtinchi qatlam — ochiqqa chiqqan bazalarni monitoring qilish. Beshinchi qatlam — operator tomonidagi himoya: zamonaviy xesh-funksiyalar, urinishlar sonini cheklash, ochiqqa chiqqan parollar ro‘yxati bilan tekshirish va g‘ayritabiiy faoliyatni aniqlash. Oltinchi qatlam — ta’lim va huquqiy ta’minot. Qatlamlardan birortasining zaifligi umumiy xavfsizlikni pasaytirishi mumkin, shu sababli ularning kompleks qo‘llanishi ilmiy jihatdan eng asosli yondashuvdir.

XULOSA

Olib borilgan tadqiqot natijalari parol xavfsizligi huquqiy, texnik va inson omillarining uyg‘unligi bilan belgilanishini ko‘rsatdi. Birinchidan, parol xavfsizligi O‘zbekiston Respublikasi Konstitutsiyasida mustahkamlangan shaxsiy hayot daxlsizligi va shaxsga doir ma’lumotlarni himoya qilish huquqining amaliy kafolati sifatida talqin qilinishi lozim; amaldagi qonunlar (“Shaxsga doir ma’lumotlar to‘g‘risida”gi, “Kiberxavfsizlik to‘g‘risida”gi, “Axborotlashtirish to‘g‘risida”gi qonunlar) umumiy huquqiy asosni yaratgan bo‘lsa-da, autentifikatsiya talablari bo‘yicha aniq texnik me’yorlar yetarlicha batafsil ishlab chiqilmagan. Ikkinchidan, ilmiy tadqiqotlar parol kuchi belgilarning xilma-xilligi bilan emas, balki uzunlik, tasodifiylik va noyoblik bilan belgilanishini, majburiy davriy almashtirish va rasmiy murakkablik qoidalarining samarasi cheklanganligini ko‘rsatadi. Uchinchidan, parollarni qayta ishlatish va ma’lumotlar sizib chiqishi hisob o‘g‘irlanishining asosiy omillari bo‘lib, kredensiallarni to‘ldirish kabi avtomatlashtirilgan hujumlar uchun zamin yaratadi. To‘rtinchidan, parol menejerlari inson omili bilan bog‘liq muammolarni sezilarli darajada kamaytiradi, ammo ularning xavfsizligi asosiy parol kuchi va menejerning kriptografik arxitekturasiga bog‘liq. Beshinchidan, ko‘p

faktorli va fishingga chidamli autentifikatsiya hisob o‘g‘irlanishi xavfini keskin kamaytiradi.

Amaliy tavsiyalar sifatida fuqarolarga har bir xizmat uchun alohida uzun parol-ibora ishlatish, parol menejerini qo‘llash, muhim hisoblarda ko‘p faktorli autentifikatsiyani yoqish, elektron pochta hisobini alohida himoyalash va tasdiqlash kodlarini hech kimga bermaslik tavsiya etiladi. Tashkilotlarga parol siyosatini ilmiy asoslangan tamoyillar asosida qayta ko‘rib chiqish, kirish huquqlarini markazlashtirilgan boshqarish va xodimlarni muntazam o‘qitish tavsiya qilinadi. Kelgusidagi tadqiqotlar parol xulq-atvorining O‘zbekiston foydalanuvchilariga xos jihatlarini va mahalliy xizmatlarda KFA hamda passkey joriy etilishi imkoniyatlarini empirik o‘rganishga qaratilishi maqsadga muvofiq.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

[1] Morris R., Thompson K. Password security: a case history // Communications of the ACM. — 1979. — Vol. 22, No. 11. — P. 594–597.

[2] O‘zbekiston Respublikasi Konstitutsiyasi (2023-yil 30-aprelda umumxalq referendumida qabul qilingan yangi tahriri), 31-modda // Milliy qonunchilik ma’lumotlari bazasi (Lex.uz). URL: https://lex.uz

[3] O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni // Milliy qonunchilik ma’lumotlari bazasi (Lex.uz). URL: https://lex.uz

[4] O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni // Milliy qonunchilik ma’lumotlari bazasi (Lex.uz). URL: https://lex.uz

[5] O‘zbekiston Respublikasining 2003-yil 11-dekabrdagi 560-II-son “Axborotlashtirish to‘g‘risida”gi Qonuni // Milliy qonunchilik ma’lumotlari bazasi (Lex.uz). URL: https://lex.uz

[6] O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son Farmoni bilan tasdiqlangan “Raqamli O‘zbekiston — 2030” strategiyasi // Milliy qonunchilik ma’lumotlari bazasi (Lex.uz). URL: https://lex.uz

[7] O‘zbekiston Respublikasi Prezidentining 2022-yil 28-yanvardagi PF-60-son Farmoni bilan tasdiqlangan “2022–2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi” // Milliy qonunchilik ma’lumotlari bazasi (Lex.uz). URL: https://lex.uz

[8] O‘zbekiston Respublikasi Jinoyat kodeksi (1994-yil 22-sentabrdagi 2012-XII-son Qonun bilan tasdiqlangan), XX¹ bob va 168-modda // Milliy qonunchilik ma’lumotlari bazasi (Lex.uz). URL: https://lex.uz

[9] Grassi P.A. et al. Digital Identity Guidelines: Authentication and Lifecycle Management. NIST Special Publication 800-63B. — Gaithersburg: National Institute of Standards and Technology, 2017. DOI: 10.6028/NIST.SP.800-63b.

[10] Bonneau J., Herley C., van Oorschot P.C., Stajano F. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes // Proceedings of the 2012 IEEE Symposium on Security and Privacy. — IEEE, 2012. — P. 553–567.

[11] Florêncio D., Herley C. A large-scale study of web password habits // Proceedings of the 16th International Conference on World Wide Web (WWW ’07). — ACM, 2007. — P. 657–666.

[12] Adams A., Sasse M.A. Users are not the enemy // Communications of the ACM. — 1999. — Vol. 42, No. 12. — P. 40–46.

[13] Bonneau J. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords // Proceedings of the 2012 IEEE Symposium on Security and Privacy. — IEEE, 2012. — P. 538–552.

[14] Weir M., Aggarwal S., Collins M., Stern H. Testing metrics for password creation policies by attacking large sets of revealed passwords // Proceedings of the 17th ACM

Conference on Computer and Communications Security (CCS ’10). — ACM, 2010. — P. 162–175.

[15] Kelley P.G., Komanduri S., Mazurek M.L. et al. Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms // Proceedings of the 2012 IEEE Symposium on Security and Privacy. — IEEE, 2012. — P. 523–537.

[16] Melicher W., Ur B., Segreti S.M. et al. Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks // 25th USENIX Security Symposium. — USENIX Association, 2016. — P. 175–191.

[17] Hitaj B., Gasti P., Ateniese G., Perez-Cruz F. PassGAN: A Deep Learning Approach for Password Guessing // Applied Cryptography and Network Security (ACNS 2019). Lecture Notes in Computer Science, vol. 11464. — Springer, 2019.

[18] Wheeler D.L. zxcvbn: Low-Budget Password Strength Estimation // 25th USENIX Security Symposium. — USENIX Association, 2016. — P. 157–173.

[19] Komanduri S., Shay R., Kelley P.G. et al. Of passwords and people: measuring the effect of password-composition policies // Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ’11). — ACM, 2011. — P. 2595–2604.

[20] Shay R., Komanduri S., Durity A.L. et al. Designing Password Policies for Strength and Usability // ACM Transactions on Information and System Security. — 2016.