ELEKTRON HUKUMATDAGI KIBERXAVFSIZLIK MUAMMOLARI: SHAXSIY MA'LUMOTLAR VA FUQAROLARNING SHAXSIY DAXLSIZLIGINI HIMOYA QILISH

Abdullayev Shohzod Xayrulla o'g'li
Chilonzor tuman adliya bo'limi bosh maslahatchisi
e-mail: shaxzodabdullayev9705@gmail.com
tel: 97 491 77 11
https://doi.org/10.5281/zenodo.11242917
Kalit so'zlar: elektron hukumat, kiber xavfsizlik, kiber hujum, shifrlash, zararli dasturlar, X-Road tizimi, E-ID tizimi.

Axborot-kommunikatsiya texnologiyalarining rivojlanishi bilan hukumatlar fuqarolari uchun yanada samarali va qulayroq xizmatlarni taklif qilish maqsadida raqamli platformalardan foydalanayotganliklari sababli, elektron hukumat tizimlarida kiberxavfsizlik masalasi muhim ahamiyat kasb eta boshladi. Elektron hukumat, davlat xizmatlarini ko'rsatish uchun raqamli vositalar va tizimlardan foydalanish, xizmatlar ko'rsatishni yaxshilash, shaffoflikni va fuqarolarning faolligini oshirish kabi ko'plab afzalliklarni taqdim etadi. Biroq, ushbu raqamli tizimlarga tobora ortib borayotgan bog'liqlik kiberxavfsizlikda ham jiddiy muammolarni keltirib chiqaradi.

Elektron hukumat tizimlari soliqlarni onlayn tarzda to'lash, ijtimoiy xizmatlardan tortib raqamli identifikatsiya tizimlari va elektron ovoz berishgacha bo'lgan keng ko'lamli xizmatlarni o'z ichiga oladi. Ushbu tizimlar orqali fuqarolarga tegishli bo'lgan shaxsiy, moliyaviy va sog'liqni saqlash bilan bog'liq ma'lumotlarini o'z ichiga olgan katta hajmdagi maxfiy ma'lumotlarni boshqaradi. Ushbu xizmatlarning raqamli tabiati va ahamiyati kiberjinoyatchilarning e'tiborini jalb qiladi va shu sababdan mazkur ma'lumotlarning yaxlitligi, mavjudligi va maxfiyligini himoya qilish uchun mustahkam kiberxavfsizlik choralarini ko'rishni talab qiladi.

Kiberxavfsizlik sohasida qator jiddiy muammaolar mavjud bo'lib quyida ularning eng asosiylari haqida fikr yuritamiz.

Ma'lumotlar tizimlarining buzilishi: Hukumatning maxfiy ma'lumotlariga ruxsatsiz kirish maxfiylikning buzilishiga va bu hukumat, davlat va fuqarolar uchun jiddiy moliyaviy zararlarga olib kelishi mumkin. Kiberjinoyatchilar ko'pincha shaxsiy ma'lumotlarni o'z ichiga olgan, darknetda sotilishi yoki boshqa shaxsiy ma'lumotlarni o'g'irlash vositasi sifatida ishlatilishi mumkin bo'lgan ma'lumotlar bazalarini nishonga olishadi.

Zararli dastur va viruslar (Ransomware): Zararli dasturlar bilan bog'liq hujumlar davlat va shaxslar uchun muhim bo'lgan ma'lumotlarni kodlash va uni shafrdan chiqarilishi uchun to'lov talab qilish orqali elektron hukumat xizmatlariga zarar yetkazishi mumkin. Bu nafaqat xizmatlarga balki hukumatning moliyaviy holatiga ham yaxshigina zarar keltiradi.

Fishing va ijtimoiy muhandislik: Kiberhujumchilar hukumat xodimlari va fuqarolarni aldash uchun tez-tez fishing va ijtimoiy muhandislik taktikalaridan foydalanadilar, bu tizimlar va ma'lumotlarga ruxsatsiz kirishga olib keladi.

Ichki tahdidlar: Maxfiy ma'lumotlarga kirish huquqiga ega bo'lgan xodimlar, agar ular o'z vakolatlarini ataylab yoki qasddan suiiste'mol qilishi ham jiddiy xavf tug'dirishi mumkin.

Eskirgan dasturiy tizimlar: Kiberhujumlarning soat sayin yangi turlari amalga oshirilmoqda. Bugungi kundan ko'pgina davlat organlari va idoralari zamonaviy xavfsizlik talablariga javob

bermaydigan texnologiyalardan foydalanishda davom etmoqda va bu ularni hujumlarga qarshi himoyasiz qolishiga olib kelmoqda.

Elektron hukumatda kiberxavfsizlikni ta'minlash bo'yicha turli davlatlarda samarali amaliyotlar yo'lga qo'yilgan. Odatda davlatlar elektron hukumat bilan bog'liq bo'lgan kiberxavfsizlik xavflarini oldini olish uchun turli strategiyalarni ishlab chiqishadi.

Jimladan, Estoniya o'zining ilg'or elektron hukumat infratuzilmasi va mustahkam kiberxavfsizlik choralari bilan mashhur. Ushbu davlat kiberxavfsizlikni mustahkamlash maqsadida quyidagi amaliyotni yo'lga qo'ygan:

X-Road tizimi: Estoniyaning X-Road xavfsiz ma'lumotlar almashinuvi tizimi bo'lib, u turli davlat ma'lumotlar bazalarini bog'laydi va xavfsiz, markazlashmagan holda ma'lumotlar uzatilishini ta'minlaydi. Ushbu tizim shifrlash va raqamli imzo kabi xavfsizlik xususiyatlari bilan ta'minlangan. Ma'lumotlar almashinuvi platformasi: Bunda yuqori xavfsizlik va maxfiylik standartlarini saqlab qolgan holda turli obyektlar o'rtasida ma'lumotlar uzluksiz almashishini ta'minlanadi[1].

E-ID tizimi: Estoniyaliklar elektron davlat xizmatlaridan foydalanish uchun xavfsiz autentifikatsiyani ta'minlovchi elektron shaxsiy kartalardan (E-ID) foydalanadilar. Elektron identifikator tizimi kuchli kriptografik standartlar bilan ta'minlangan bo'lib, fuqarolar ma'lumotlarini himoya qilishni ta'minlaydi.

Doimiy kibertayyorgarliklar: Estoniya o'zining elektron hukumat tizimlarining kibertahdidlarga chidamliligini sinab ko'rish uchun "Kiberkoalitsiya" mashg'ulotlari kabi muntazam kibermashqlar o'tkazib boradi. Estoniya 2018-yildan buyon National Cyber Security Index da 1-o'rinni egallagan[2]. International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI) da esa 5-o'rinni qayd etgan[3].

Davlat-xususiy sheriklik: Estoniya hukumati mudofaa qobiliyatini oshirish uchun xususiy sektordagi kiberxavfsizlik sohasidagi tashkilotlar bilan yaqindan hamkorlikni amalga oshirib keladi.

Singapur davlat ham Osiyo-Tinch okeani mintaqasida kiberxavfsizlik bo'yicha yetakchi o'rinni egallaydi. Uning strategiyasining asosiy tarkibiy qismlari quyidagilardan iborat:

Kiberxavfsizlik to'g'risidagi qonun: Singapurning Kiberxavfsizlik to'g'risidagi qonuni muhim axborot infratuzilmasini, jumladan, elektron hukumat tizimlarini himoya qilish uchun tartibga soluvchi huquqiy bazani shakllantirib bergan. U muntazam ravishda xavflarni baholab borish vaholat haqida doimiy hisobot berishni talab qiladi.

Kiberxavfsizlik agentligi (CSA): CSA milliy kiberxavfsizlik strategiyalarining amalga oshirilishini nazorat qiladi va turli sektorlar, jumladan, davlat xizmatlari bo'yicha sa'y-harakatlarni ham muvofiqlashtiradi. (CSA) 2015-yilda Singapur raqamli infratuzilmasining kiberxavfsizligini nazorat qilish va ta'minlash maqsadida tashkil etilgan davlat organi. CSAning

[1] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Estonia-ranks-fifth-in-the-global-cybersecurity-index.aspx) [[]](https://e-estonia.com/estonia-takes-the-top-spot-in-the-national-cyber-security-index/).

[2] https://estonianworld.com/security/estonia-ranks-first-in-the-world-in-the-national-cyber-security-index/) [[❞]](https://e-estonia.com/estonia-takes-the-top-spot-in-the-national-cyber-security-index/).

[3] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Estonia-ranks-fifth-in-the-global-cybersecurity-index.aspx).

asosiy maqsadi kibermakonda Singapur milliy xavfsizlikni ta'minlash himoya qilish va raqamli iqtisodiyotni qo'llab-quvvatlashdir[4].

Kiberxavfsizlik bo'yicha kadrlarni tayorlash: Singapur elektron hukumat platformalarini boshqarish va himoya qilish uchun malakali mutaxassislar bilan ta'minlab, Cybersecurity Associates and Technologists (CSAT)[5] dasturi kabi tashabbuslar orqali kiberxavfsizlik bo'yicha iste'dodli kadrlarni yetishtirishga katta mablag' sarflaydi.

Kengaytirilgan tahdidlarni aniqlash: Singapur real vaqt rejimida kibertahdidlarni aniqlash va kamaytirish uchun ilg'or tahdidlarni aniqlash tizimlari va sun'iy intellektdan foydalanadi.

Natijada bugungi kunda Singapur yaxshi rejalashtirilgan kiberxavfsizlik mexanizmi va imkoniyatlarini sezilarli darajada oshirishga muvaffaq bo'lgan.

Amerika Qo'shma Shtatlari elektron hukumat tizimlarida kiberxavfsizlik bo'yicha ko'p bosqichli yondashuvni qo'llaydi, bunda muvofiqlashtirish va barqarorlikni ta'kidlaydi.

Kiberxavfsizlik va infratuzilma xavfsizligi agentligi (CISA): CISA mamlakatning jismoniy va kiber infratuzilmasini himoya qilish va barqarorligini oshirish bo'yicha milliy sa'y-harakatlarni boshqaradi. U federal, shtat va mahalliy hokimiyat organlariga yo'l-yo'riq va ko'rsatmalar beradi.

The Continuous Diagnostics and Mitigation (CDM) dasturi: CDM dasturi federal agentliklarga kiberxavfsizlik holatini yaxshilash uchun vositalar va xizmatlarni taklif qiladi. Uning faoliyati doimiy monitoring qilish, zaifliklarni aniqlash va hujumlarga javob berishga qaratilgan. Ushbu dastur (CDM) 2012-yilda ishlab chiqilgan federal hukumat tarmoqlari va tizimlarining kiberxavfsizlik holatini yaxshilash uchun mo'ljallangan.

Xavf va avtorizatsiyani boshqarish bo'yicha federal dastur (FedRAMP): FedRAMP federal agentliklar tomonidan foydalaniladigan bulut xizmatlari xavfsizligini baholash, avtorizatsiya qilish va doimiy monitoringini amalga oshirish hamda elektron hukumat dasturlarini qat'iy xavfsizlik standartlariga mos kelishini ta'minlaydi.

Avstraliyaning elektron hukumatning kiberxavfsizlikka bo'lgan yondashuvi qonunchilik, tashkiliy va texnik choralarni o'z ichiga olgan integratsiyalashgan strategiyani o'z ichiga oladi.

Kiberxavfsizlik strategiyasi 2020: Avstraliyaning Kiberxavfsizlik strategiyasi o'n yil davomida mamlakatning kibermudofaasini kuchaytirishga qaratilgan keng qamrovli reja bo'lib, 1,67 milliard dollar sarmoya ajratilgan[6] hamda barcha sektorlarda, jumladan, elektron hukumatda kiberxavfsizlikni kuchaytirishga qaratilgan kompleks yondashuvni belgilaydi. Bunda o'zaro hamkorlik, imkoniyatlarni rivojlantirish va xalqaro hamkorlikka urg'u beriladi.

Avstraliya kiberxavfsizlik markazi (ACSC): ACSC kiberxavfsizlik masalalari bo'yicha axborot almashish va hamkorlik qilish uchun markaziy richag vazifasinio'taydi, davlat idoralarini raqamli infratuzilmasini himoya qilishni amalga oshiradi.

Ma'lumotlarning buzilishi haqida majburiy bildirishnoma: Avstraliya qonunchiligi tashkilotlardan, jumladan, davlat idoralaridan zarar ko'rgan shaxslarni va ACSCni jiddiy

[4] https://www.csa.gov.sg/News-Events/Press-Releases/2024/csa-releases-key-findings-from-singapore-cybersecurity-health-report-2023) [[❞]](https://opengovasia.com/2024/03/29/singapore-insights-from-csas-first-cybersecurity-report/).

[5] https://www.csa.gov.sg) [[❞]](https://www.csa.gov.sg/our-programmes/talents-skills-development/sg-cyber-talent).

[6] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australias-cyber-security-strategy-2020) [[❞]](https://www.rusi.org/explore-our-research/publications/commentary/australias-cyber-security-strategy/).

zararga olib kelishi mumkin bo‘lgan ma’lumotlar buzilishi haqida zudlik bilan xabardor qilishni talab qiladi, bu esa shaffoflik va javobgarlikni ta’minlaydi.

Xavfsiz bulutli strategiya: Avstraliya bulutli provayderlarning qat’iy xavfsizlik talablariga javob berishini ta’minlab, hukumat dasturlari uchun xavfsiz bulut xizmatlaridan foydalanishni targ‘ib qiladi.

Shaxsiy ma’lumotlar va fuqarolarning shaxsiy daxlsizligini himoya qilish

Elektron hukumatdagi kiberxavfsizlik muammolarini hal qilish uchun mamlakatlar texnologik, tashkiliy va huquqiy choralarni o‘z ichiga olgan ko‘p qirrali yondashuvni qo‘llashlari kerak. Quyidagi strategiyalar shaxsiy ma’lumotlar va fuqarolarning daxlsizligini himoya qilishga yordam beradi:

Birinchidan, texnologik chora-tadbirlar:

Shifrlash*:* Kuchli shifrlashdan foydalanish ma’lumotlarni uzatish va saqlash vaqtida xavfsiz bo‘lishini ta’minlaydi. Bu maxfiy ma’lumotlarni ruxsatsiz kirishdan himoya qilish uchun zarurdir.

***Ko‘p bosqichli autentifikatsiya (MFA)*:** Elektron hukumat xizmatlariga kirish uchun ko‘p bosqichli autentifikatsiyani qo‘llash xavfsizlikni ta’minlashga qo‘shimcha imkoniyat yaratadi, hakerlarga buzib kirishni qiyinlashtiradi.

Doimiy xavfsizlik nazorati va tekshiruvi: muntazam xavfsizlik tekshiruvlari va zaifliklarni aniqlash elektron hukumat tizimlaridagi mavjud mumkin bo‘lgan kamchiliklarni aniqlash va bartaraf etishga yordam beradi.

Endpoint Security tizimi: Barcha mijoz qurilmalariga masofadan ulangan kompyuter tarmoqlarini, jumladan, davlat xodimlari tomonidan foydalaniladigan kompyuterlar va mobil qurilmalarni zararli dasturlardan va boshqa tahdidlardan himoyalanganligini ta’minlashda juda muhim.

Kengaytirilgan tahdidlarni aniqlash va javob berish: real vaqt rejimida kibertahdidlarni aniqlash va ularga javob berish uchun sun’iy intellektdan foydalanish elektron hukumat tizimlari xavfsizligini sezilarli darajada oshirishi mumkin.

Ikkinchidan, tashkiliy chora-tadbirlar.

Kiberxavfsizlik bo‘yicha trening va xabardorlik: Kiberxavfsizlik bo‘yicha eng yaxshi amaliyotlar va tahdidlardan xabardorlik bo‘yicha davlat xodimlari uchun muntazam trening dasturlari muhim ahamiyatga ega. Xodimlarni fishing va boshqa ijtimoiy muhandislik taktikalarini farqlay olishga o‘rgatish hujumlarning muvaffaqiyatli amalga oshirilishi xavfini kamaytirishi mumkin.

Davlat-xususiy sheriklik: Kiberxavfsizlik bo‘yicha xususiy sektor mutaxassislari bilan hamkorlik qilish davlat idoralariga tahdidlar haqidagi so‘nggi razvedka ma’lumotlari va mudofaa texnologiyalaridan foydalanish imkoniyatini beradi.

Uchinchidan, huquqiy va tartibga soluvchi chora-tadbirlar.

Ma’lumotlarni himoya qilish to‘g‘risidagi qonunlar: Shaxsiy ma’lumotlarni to‘plash, foydalanish va saqlashni tartibga soluvchi ma’lumotlarni himoya qilish bo‘yicha keng qamrovli huquqiy asoslarni ishlab chiqish fuqarolarning shaxsiy daxlsizligini va elektron davlat xizmatlariga ishonchni oshirishi mumkin. Ushbu qonunlar ma’lumotlarni minimallashtirish, shaxsiy ma’lumotlarga kirishda foydalanuvchi roziligi huquqini o‘z ichiga olishi mumkin.

Majburiy buzilish to‘g‘risida bildirishnoma: yuqorida aytib o‘tilganidek, davlat organlaridan zarar ko‘rgan shaxslarni va tegishli organlarni ma’lumotlar buzilishi haqida xabardor qilishni talab qilish shaffoflik va javobgarlikka yordam beradi.

Xalqaro hamkorlik: Kibertahdidlar ko‘pincha global xarakterga ega bo‘lib, xalqaro hamkorlikni talab qiladi. Boshqa mamlakatlar bilan kiberjinoyatlar bo‘yicha ma’lumotlar va ilg‘or tajribalarni almashish elektron hukumat tizimlarining umumiy xavfsizlik holatini yaxshilashi mumkin.

Xulosa o‘rnida shuni aytish mumkinki, elektron hukumatdagi muvaffaqiyatli kiberxavfsizlik amaliyotlarini amalga oshirish fuqarolarning elektron davlat xizmatlaridan ishonch bilan foydalanishini ta’minlaydi. Bunga yuqorida keltirganimizdek Estoniyaning X-Road va e-ID tizimlari xavfsiz elektron hukumat infratuzilmasining namunali modellaridir misol qilish mumkin. X-Road platformasi shifrlash va kirishni boshqarishning yuqori darajasini saqlab, davlat ma’lumotlar bazalari o‘rtasida xavfsiz ma’lumotlar almashinuvini ta’minlaydi. Elektron identifikatsiya tizimi xavfsiz autentifikatsiya va raqamli imzolarni qo‘llash imkonini beradi.

References:

1. https://www.itu.int/en/ITU-D/Cybersecurity/ Pages/Estonia-ranks-fifth-in-the- global-cybersecurity-index.aspx) (https:// e-estonia. com/estonia-takes-the-top-spot-in-the-national-cyber-security-index/).
2. https://estonianworld.com/security/estonia-ranks-first-in-the-world-in-the-national-cyber-security-index/) [[”]](https://e-estonia.com/estonia-takes-the-top-spot-in-the-national-cyber-security-index/).
3. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Estonia-ranks-fifth-in-the-global-cybersecurity-index.aspx).
4. https://www.csa.gov.sg/News-Events/ Press-Releases/2024/csa-releases-key-findings -from- singapore- cybersecurity-health-report-2023) [[”]](https://opengovasia.com/2024/03/29/singapore-insights-from-csas-first-cybersecurity-report/).
5. https://www.csa.gov.sg) [[”]](https://www.csa.gov.sg/our-programmes/talents-skills-development/sg-cyber-talent).
6. https://www.homeaffairs.gov.au /about-us/our-portfolios/cyber-security/strategy /australias-cyber-security-strategy-2020) (https://www.rusi.org/ explore-our-research/publications/commentary/australias-cyber-security-strategy/).