“O‘ZBEKISTON MILLIY ELEKTR TARMOQLARI” AKSIYADORLIK JAMIYATI

АКЦИОНЕРНОЕ ОБЩЕСТВО “НАЦИОНАЛЬНЫЕ ЭЛЕКТРИЧЕСКИЕ СЕТИ УЗБЕКИСТАНА”

BUYRUQ
ПРИКАЗ

«03» 07 2025-yil 131-son Toshkent sh.

“O‘zbekiston MET” AJning Axborot xavfsizligi siyosati to‘g‘risida

O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida” 2022-yil 15-apreldagi O‘RQ-764-son Qonuni va Jamiyatda axborot va kiberxavfsizlikni ta’minlash bo‘yicha 2025-yilga mo‘ljallangan chora-tadbirlar rejasiga muvofiq Jamiyat Axborot xavfsizligi siyosatini amalga kiritish va xodimlarni tanishtirish maqsadida,

BUYURAMAN:

1. “O‘zbekiston MET” AJning Axborot xavfsizligi siyosati Davlat xavsizligi xizmatining 2025-yil 15-maydagi 14/7293-son xati va Raqamli texnologiyalar vazirligining 2021-yil 31-martdagi 27-8/2282-son xati asosida kelishilganligi ma’lumot uchun qabul qilinsin.

2. ““O‘zbekiston milliy elektr tarmoqlari” AJning Axborot xavfsizligi siyosati” ilovaga muvofiq tasdiqlansin.

3. Axborot va kiberxavfsizlik bo‘limi (Tashtayev) va barcha filial rahbarlariga:

3.1 “O‘zbekiston milliy elektr tarmoqlari” AJning Axborot xavfsizligi siyosati Jamiyat markaziy apparati va barcha filial xodimlari (shu jumladan, ishga yangi qabul qilingan xodimlar)ni maxsus jurnalga imzo qo‘yish orqali tanishtirish hamda mazkur hujjatning mazmun va mohiyati, belgilangan talablari bo‘yicha muntazam tushuntirish ishlarini olib borsin;

3.2 Zarur hollarda “O‘zbekiston MET” AJning muhim axborot infratuzilmasi hamda axborotlashtirish obyektlarida axborot xavfsizligi ichki

auditini o‘tkazsin.

4. Belgilangsinki, “O‘zbekiston MET” AJ Axborot xavfsizligi siyosati talablarini buzish xolati mehnat intizomining buzilishi sifatida baholanib, aybdor xodimga nisbatan ichki mehnat tartibi qoidalariga muvofiq ta’sir chorasi qo‘llaniladi.

5. Ishlarni yuritish va xo‘jalik boshqarmasi (Mirzaraimova) Axborot xavfsizligi siyosatidan ko‘chirma barcha filiallarga tarqatilishini ta’minlasin.

6. Mazkur buyruq ijrosining nazorati boshqaruv raisining birinchi o‘rinbosari S. Artikov zimmasiga yuklatilsin.

Boshqaruv raisi **D. Isaqulov**

Tarqatiladi: Barcha bosh boshqarma, boshqarma, xizmat, bo‘lim hamda filiallarga

Ijrochi: AKB
Tel.: 32-377

"O'zbekiston MET" AJning
2025-yil 03-iyul
131 - son buyrug'iga
ilova

"O'zbekiston MET" AJ xodimlarini Axborot xavfsizligi siyosati bilan tanishtirish uchun ko'chirma.

1. Axborot xavfsizligini ta'minlash bo'yicha xodimlarga qo'yiladigan talablar

"O'zbekiston milliy elektr tarmoqlari" AJ *(keyingi o'rinlarda - Jamiyat)* ning Axborot xavfsizligi siyosatiga rioya qilish uchun xodimlar quyidagi talablarni bajarishlari shart:

Jamiyatning yangi xodimlariga nisbatan, axborot xavfsizligi bo'yicha kirish yo'riqnoma o'tkazilishi kerak.

Belgilar va qisqartmalar

Ushbu Siyosatda quyidagi belgilar va qisqartmalardan foydalanilgan:
AD (Active Directory) – domen uchun ajratilgan tizim;
VPN (virtual private network) – shaxsiy himoyalangan tarmoq;
XDFU – xizmat doirasida foydalanish uchun;
AKT – axborot-kommunikatsiya texnologiyalari;
IMUT –idoralararo ma'lumot uzatish tarmog'i;
AKHV – axborotni kriptografik himoyalash vositalari;
AXBT – axborot xavfsizligini boshqarish tizimi;
MBBT – ma'lumotlar bazasini boshqarish tizimi;
ERI – elektron raqamli imzo.

Axborot xavfsizligi administratori – (Axborot va kiberxavfsizlik bo'limi);
Lokal tarmoq administratori – (Raqamlashtirish boshqarmasi);
Mintaqaviy axborot xavfsizligi administratori – (Filiallardagi administrator).

1.1. Himoyalangan ma'lumotlarga ishlov berish tartibi

Ushbu tartib O'zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 16-oktabrdagi 295-sonli "O'zbekiston Respublikasida axborotlashtirish obyektlarida konfidensial ma'lumotlarni tashkil etish va xavfsizligini ta'minlash to'g'risidagi nizomni tasdiqlash to'g'risida"gi qarori va O'zbekiston Respublikasi Bosh vazirining o'rinbosari davlat sirlarini saqlash bo'yicha idoralararo komissiya raisi tomonidan 2006-yil 5-dekabrda tasdiqlangan - tarqatilishi cheklangan ma'lumotlarga ega hujjatlar, fayllar va nashrlarni ro'yxatga olish, ishlov berish va saqlash tartibi to'g'risidagi yo'riqnomaga asosan ishlab chiqilgan.

1. Quyidagilar himoya qilinadi va tarqatilmaydi:

- Jamiyatning konfidensial ma'lumotlari ro'yxatiga kiritilgan, hujjatlashtirilgan axborotlar;

- tarqatilishi cheklangan konfidensial bo‘lmagan ma’lumotlarga ega bo‘lgan hujjatlar, fayllar va nashrlar.

2. Tarqatilishi cheklangan konfidensial bo‘lmagan ma’lumotni o‘z ichiga olgan hujjatlar, fayllar va nashrlar O‘zbekiston Respublikasi Bosh vazirining o‘rinbosari - Davlat sirlarini saqlash bo‘yicha idoralararo komissiya raisi tomonidan 2006-yil 5-dekabrda tasdiqlangan tarqatilishi cheklangan ma’lumotlarga ega bo‘lgan hujjatlar, fayllar va nashrlarni hisobga olish, ishlov berish va saqlash tartibi to‘g‘risidagi yo‘riqnomaga muvofiq belgilanadi.

Tarqatilishi cheklangan ma’lumotlarga O‘zbekiston matbuot va axborot agentligi tomonidan e’lon qilinishi taqiqlangan ma’lumotlarning ro‘yxati, Jamiyat va boshqa vazirliklar va idoralarning ochiq matbuotda, radio va televizion ko‘rsatuvlarda e’lon qilinishi taqiqlangan ma’lumotlar ro‘yxati, shuningdek oshkor qilinmagan ma’lumotlar, ochiq e’lon qilinishi O‘zbekiston Respublikasiga zarar yetkazishi mumkin bo‘lgan boshqa ma’lumotlar kiradi.

Himoyalanadigan ma’lumot bilan ishlashga qo‘yiladigan talablar

Jamiyatning konfidensial ma’lumotlari ro‘yxatini shakllantirish, yuritish va o‘z xodimlariga yetkazish ustidan nazoratni Axborot va kiberxavfsizlik bo‘limi boshlig‘i amalga oshiradi.

Jamiyatning konfidensial ma’lumotlarini, shu jumladan axborot resurslarida himoya qilish bo‘yicha ishlarni tashkil etish va amalga oshirish, O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 16-oktyabrdagi 295-sonli qarori talablariga muvofiq amalga oshiriladi.

Jamiyatning konfidensial ma’lumotlari ro‘yxatiga kiritilgan konfidensial ma’lumotlarni tarqatmaslik ustidan nazorat Axborot va kiberxavfsizlik bo‘limi tomonidan amalga oshiriladi.

Axborot resursining ishlashi davomida konfidensial ma’lumotlarning himoyasini ta’minlash uchun quyidagi asosiy talablarga rioya qilish kerak:

- muhofaza qilinadigan axborotni qayta ishlash obyektlari joylashgan binoda faqat qayta ishlangan ma’lumotlarga ruxsat berilgan shaxslar bo‘lishi mumkin;

- boshqa profilaktika va ta’mirlash ishlarini olib borish uchun muhofaza qilinadigan binolarga boshqa shaxslarni qabul qilish faqat Jamiyat rahbarining ruxsati bilan amalga oshirilishi lozim.

Konfidensial ma’lumotlarni faqat boshqariladigan hudud ichida joylashgan ajratilgan lokal tarmoqlarda ishlash mumkin. Axborotlashtirish obyektlari masofaviy bo‘lganda, O‘zbekiston Respublikasida sertifikatlangan kriptografik ma’lumotlarni himoya qilish vositalaridan foydalanish kerak.

Jamiyat axborot resurslarida mavjud bo‘lgan konfidensial ma’lumotlarni himoya qilish va tarqatmaslik ustidan nazorat Axborot va kiberxavfsizlik bo‘limi boshlig‘i tomonidan amalga oshiriladi.

Ushbu tartibning 2-bandida ko‘rsatilgan tarqatilishi cheklangan konfidensial bo‘lmagan ma’lumotlarni o‘z ichiga olgan hujjatlar, fayllar va nashrlarda “XDFU” muhri, hujjat va nashrlarda qo‘shimcha ravishda nusxalari soni qo‘yiladi.

“XDFU” muhrini bosish zarurligini aniqlash ushbu tartibning 2-bandida ko‘rsatilgan ro‘yxatlar asosida amalga oshiriladi: hujjat bo‘yicha - ijrochi va hujjatni imzolagan shaxs, nashrda esa - muallif va nashrni nashrga tasdiqlovchi rahbar.

Tarqatilishi cheklangan ma'lumotlarini o'z ichiga olgan hujjatlar, fayllar va nashrlar boshqa jurnallardan alohida jurnallarda ro'yxatga olinishi kerak, unda nusxalar soni, hujjat varaqlari soni va hujjatga qo'shimchalar ko'rsatilishi kerak.

Qog'ozda tarqatilishi cheklangan ma'lumotlar bo'lgan hujjatlarni ularning ijrochilariga va ijrochilar o'rtasida o'tkazish ro'yxatga olish va nazorat shakllarida imzolangan holda amalga oshiriladi.

Tarqatilishi cheklangan ma'lumotlarni o'z ichiga olgan hujjatlar:

- belgilangan tartibda qonun hujjatlari talablariga muvofiq ta'minlangan, aloqa kanallari, kuryerlik aloqalari yoki kuryerlik uzatish orqali yuboriladi. Cheklangan tarqatish, kuryerlik xizmati yoki kuryer transferi to'g'risidagi rasmiy ma'lumotlarni o'z ichiga olgan hujjatlar yuborilgan taqdirda, qalin qog'ozdan qilingan konvertlar (paketlar) ishlatiladi. Bunday hujjatlarni yuborishda boshqaruv obyektlarining ish yuritish bo'limlari va hududiy bo'linmalarning xodimlari ularni qog'ozga oldindan o'rab, keyin konvertlarga soladilar. Konvertning yuqori qismiga muhrning izi qo'yiladi;

- seyflarda, qulflanadigan shkaflarda, javonlarda yoki stol tortmasida saqlanadi, bunda uchinchi shaxslarning hujjatlarga kirish huquqi bundan mustasno.

Takrorlangan hujjatlarni ro'yxatga olish birma-bir amalga oshiriladi.

Tarqatilishi cheklangan hujjatlarning elektron nusxalari boshqa axborot tashuvchi vositalarga faqat Jamiyat rahbariyatining yozma ruxsati (qarori) bilan o'tkazilishi mumkin. Bunday holda, hujjatning elektron matnida "Rasmiy foydalanish uchun" cheklovchi muhri va nusxasi raqami qo'yiladi.

Tarqatilishi cheklangan ma'lumotlari bo'lgan hujjatlar, fayllar va nashrlarni hisobga olish, takrorlash, saqlash, foydalanish, saqlash va yo'q qilish uchun tanlash Jamiyat xodimlari tomonidan 2006-yil 5-dekabrda O'zbekiston Respublikasi Bosh vazirining o'rinbosari - davlat sirlarini saqlash bo'yicha idoralararo komissiya raisi tomonidan tasdiqlangan, tarqatilishi cheklangan ma'lumotlarga ega bo'lgan hujjatlar, fayllar va nashrlarni ro'yxatga olish, ishlov berish va saqlash tartibi to'g'risidagi yo'riqnomaga muvofiq amalga oshiriladi.

Jamiyatning "XDFU" tamg'asi bo'lgan hujjatlar, fayllar va nashrlar bilan ishlovchi xodimlari ushbu Tartib va 2006-yil 5-dekabrda O'zbekiston Respublikasi Bosh vazirining o'rinbosari - davlat sirlarini saqlash bo'yicha idoralararo komissiya raisi tomonidan tasdiqlangan, tarqatilishi cheklangan ma'lumotlarga ega bo'lgan hujjatlar, fayllar va nashrlarni ro'yxatga olish, ishlov berish va saqlash tartibi to'g'risidagi yo'riqnoma bilan tanishishlari kerak.

Jamiyat tarkibiy bo'linmalari rahbarlari va tegishli mansabdor shaxslar hujjatlar, fayllar va nashrlarning "XDFU" tamg'asi bo'lgan ma'lumotlarning to'g'ri saqlanishini, ko'payishi va ishlatilishini, hujjatlar, fayllar va nashrlarni yozib olish, ishlov berish va saqlash tartibi to'g'risidagi yo'riqnomaning talablariga, shuningdek 2006-yil 5-dekabrdagi O'zbekiston Respublikasi Bosh vazirining o'rinbosari - davlat sirlarini saqlash bo'yicha idoralararo komissiya raisi tomonidan tasdiqlangan, tarqatilishi cheklangan ma'lumotlarga ega bo'lgan hujjatlar, fayllar va nashrlarni ro'yxatga olish, ishlov berish va saqlash tartibi to'g'risidagi yo'riqnoma talablariga, rioya etilishi uchun javobgar.

Jamiyat xodimlari Jamiyatning 2022-yil 29-iyundagi 155-sonli buyrug'i bilan tasdiqlangan Jamiyat markaziy apparatida "tarqalishi cheklangan maxfiy bo'lmagan ma'lumotlarni o'z ichiga olgan hujjatlar, jildlar va nashrlarni (XDFU "xizmatda

doirasida foydalanish uchun" belgisi mavjud bo'lgan) hisobga olish, muomalada bo'lish va saqlash tartibi to'g'risida"gi yo'riqnoma talablari bilan tanishgan bo'lishlari shart.

Jamiyat xodimlari kasbiy faoliyati davomida o'zlariga ma'lum bo'lgan axborotning saqlanishini va konfidensialligini ta'minlash yuzasidan barcha choralarni ko'rishlari shart, ularning oshkor etilganligi uchun ular qonun hujjatlarida belgilangan tartibda javob beradilar.

Jamiyatda xodimlar XDFU (xizmat doirasida foydalanish uchun) turdagi axborotni qayta ishlash, saqlash, foydalanishga mo'ljallangan vositalar sifatida maxsus USB xotiralardan foydalaniladi. Ushbu USB xotira foydalanuvchiga inventar raqami bo'yicha mas'ul shaxsga biriktirilgan. Jamiyatning Ishlarni yuritish boshqarmasi xodimlari tomonidan USB xotiraga mas'ul shaxsning imzosi asosida XDFU belgisi bo'lgan hujjatlarni elektron ko'rinishdagi nusxalari yozib beriladi. XDFU belgisi bo'lgan hujjatlarning electron nusxalarini ular tayyorlangan va chop etilgandan keyin ish stansiyalari va boshqa electron tashuvchilarida (XDFU uchun ajratilgan USB tashuvchilardan tashqari) qoldirish va saqlash taqiqlanadi.

1.2. Internet tarmog'i resurslaridan foydalanish va korporativ elektron pochtasi bilan ishlash bo'yicha chora-tadbirlar

Asosiy qoidalar

Ushbu yo'riqnoma Jamiyat va tizim korxonalar xodimlari tomonidan internetdan foydalanish va korporativ elektron pochta bilan ishlash tartibi va talablarini belgilaydi.

1. Jamiyatning cheklangan miqdordagi xodimlariga o'zlarining xizmat vazifalarini bajarish uchun tashqi axborot manbalariga to'g'ridan-to'g'ri internetga ulanish imkoniyati beriladi.

Elektron pochta xizmatlari Jamiyat xodimlariga faqat o'z xizmat vazifalarini bajarishlari uchun beriladi. Shaxsiy maqsadlarda foydalanish qat'iyan taqiqlanadi.

Elektron pochta Jamiyatning barcha xodimlariga ochib beriladi.

2. Jamiyat xodimlari tomonidan internetga kirish, shuningdek ularni korporativ elektron pochtaga ulash tarkibiy bo'linma rahbari tomonidan amalga oshirilishi mumkin.

Xodim ishlaydigan tarkibiy bo'linma rahbarining va Axborot xavfsizligi administratorining Jamiyatning mintaqaviy axborot xavfsizligi administratorlari roziligisiz mustaqil ravishda internetga qo'shimcha ulanish va korporativ elektron pochtalarga ulanish nuqtalarini tashkil etish taqiqlanadi.

3. Jamiyat xodimlariga internet va korporativ elektron pochtalarga texnik kirish Raqamlashtirish boshqarmasi (tarmoq administratori) va tizim korxonalari administratorlari bilan birgalikda ta'minlanadi.

Korporativ elektron pochta matnli xabarlar yoki elektron shakldagi hujjatlar shaklida xizmat ma'lumotlarini almashish uchun ishlatiladi. Konfidensial ma'lumotlar elektron pochta orqali, uning konfidensialligi va yaxlitligini ta'minlagan holda, xususan, E-xat himoyalangan elektron pochta tizimi orqali uzatilishi shart.

Korporativ elektron pochtaga kirish huquqiga ega bo‘gan xodim unikal pochta manzilini oladi. Elektron pochta manzili Jamiyat va uning tizim korxonalari administratorlari tomonidan foydalanuvchi akkauntiga binoan beriladi.

4. Jamiyatga tegishli bo‘lgan har qanday konfidensial ma’lumotni mesenjerlardan, shuningdek internetdagi boshqa ma’lumotlar almashish tizimlari (tezkor xabar almashish tizimlari, ijtimoiy tarmoqlar va boshqa tizimlar, shu jumladan har qanday turdagi elektron-pochta) orqali uzatish taqiqlanadi.

5. Jamiyat xodimlari uchun internetga va korporativ elektron pochtaga kirish Raqamlashtirish boshqarmasi (lokal tarmoq administratori) tomonidan ta’minlanadi.

6. Internetga kirish ish stansiyasidan amalga oshiriladi. Boshqa shaxsning ishchi stansiyasidagi harakatlar uchun javobgarlik ushbu harakat amalga oshirilgan ishchi stansiyasi biriktirilgan xodim zimmasiga yuklatiladi.

7. Jamiyat xodimlari tomonidan internet va korporativ elektron pochtadan foydalanish tartibi Axborot va kiberxavfsizlik bo‘limi tomonidan nazorat qilinadi, shuningdek xodimlarning lavozim yo‘riqnomalarida belgilanadi.

8. Internet tarmog‘i foydalanuvchilarining tarmoqda ish faoliyatini NethServer (OpenSource) ochiq kodli dasturiy ta’minoti yordamida nazorat qilinadi. Loglar asosida quyidagi parametrlar bo‘yicha tahlil o‘tkaziladi:

- ishlatilgan manbalar ro‘yxati;
- trafik hajmi.

Internet foydalanuvchilari uchun asosiy talablar

1. Internetdan foydalanganda quyidagilar zarur:

- ushbu qo‘llanmaning talablariga, shuningdek Jamiyatning axborot xavfsizligini ta’minlashga oid boshqa me’yoriy-huquqiy hujjatlarga rioya qilish;
- internetdan faqat o‘z xizmat vazifalarini bajarish uchun foydalanish;
- Axborot xavfsizligi administratorlariga (tizim korxonalari administratorlariga) ushbu qo‘llanma talablari buzilganligi to‘g‘risida xabar berish;
- o‘zlarining identifikatsiya ma’lumotlarini (parollar va boshqalar) sir saqlash, uchinchi shaxslarga identifikatsiya ma’lumotlarini bermaslik yoki oshkor qilmaslik.

2. Jamiyat xodimlari internetdan quyidagi maqsadlarda foydalanish huquqiga ega:

- Internetdagi axborot resurslariga kirish orqali o‘zlarining ish faoliyatiga oid vazifalarini bajarish uchun zarur bo‘lgan har qanday ma’lumotni internet tarmog‘idan olish;
- uchinchi tomon tashkilotlari (ishtirokchilar, pudratchilar, ijrochilar va boshqalar) bilan o‘zaro aloqalar;
- xodim o‘z vazifalarini va boshqa rasmiy vazifalarini rahbarlar tomonidan belgilangan muddatlarda qat’iy bajarishi sharti bilan, o‘z bilim va malakasini oshirish yuzasidan shuningdek, O‘zbekistonning ijtimoiy-siyosiy va ijtimoiy-iqtisodiy hayoti bilan tanishish, respublikadagi va dunyodagi so‘nggi voqealar to‘g‘risida ma’lumot olish;
- Jamiyat xodimlari onlayn xizmatlardan foydalanish, xususan, chiptalarni sotib olish, mehmonxonalarni bron qilish, viza olish va h.k.

- xizmat safarlari, xorijiy vakillarni qabul qilish, Jamiyat tomonidan o‘tkaziladigan boshqa tadbirlarni o‘tkazish bilan bog‘liq tashkiliy masalalarni hal qilish;

- Jamiyatda foydalanilayotgan dasturiy ta’minotlarni o‘z vaqtida yangilash va h.k.

3. Quyidagi hollarda internetdan foydalanish taqiqlanadi:

- internetdan shaxsiy yoki ko‘ngilochar maqsadlarda foydalanish;
- xodimlarga internetga ruxsatsiz ulanish imkoniyatini beradigan maxsus jihoz va dasturlardan foydalanish;
- Jamiyat lokal tarmog‘i elementlarining normal ishlashini buzishga qaratilgan har qanday harakatlarni bajarish;
- internetda ishlashda tashqi proksi-serverlar (anonimayzerlar, TOR tarmoqlari, tashqi VPN serverlar)dan foydalanish;
- Jamiyat korporativ elektron pochta manzillarini e’lonlarda, konferensiyalarda va mehmonlar kitoblarida e’lon qilish;
- xizmat ma’lumotlarini yuborish uchun korporativ bo‘lmagan elektron pochtadan foydalanish;
- konfidensial ma’lumotlarni yuborish uchun shaxsiy elektron pochta, ijtimoiy tarmoqlar va tezkor xabar almashish tizimlaridan foydalanish;
- foydalanuvchi ma’lumotlari va parollarini uzatish;
- tarmoq yukini oshiradigan va boshqa foydalanuvchilarning normal ishlashiga xalaqit beradigan video va audio oqimlarning uzatiladigan manbalardan foydalanish;
- shubhali manbalarga, shu jumladan quyidagi toifadagi saytlarga tashrif buyurish:
- onlayn kazinolar;
- o‘yinlar;
- tanishuv saytlari;
- O‘zbekiston Respublikasi Oliy sudi tomonidan internet jahon tarmog‘idagi diniy ekstremistik, terroristik va aqidaparastlik g‘oyalari bilan yo‘g‘rilgan deb topilgan hamda O‘zbekiston Respublikasining hududiga olib kirish, tayyorlash, saqlash, tarqatish va namoyish etilishi taqiqlangan manbaa va kontentlar (materiallar) ro‘yxati;
- O‘zbekiston Respublikasining amaldagi qonunchiligi bilan taqiqlangan qaroqchilik (pirat) va pornografik kontentni tarqatish saytlari;
- ekstremistik tashkilotlar saytlari;
- mayning saytlari;
- har qanday kriptovalyuta;
- bukmekerlik saytlari;
- internetda noqonuniy operatsiyalarni amalga oshirish va qonun hujjatlariga, shuningdek ushbu qo‘llanmaga zid bo‘lgan boshqa harakatlarni bajarish.

4. Jamiyat xodimlari quyidagi huquqlarga ega:

- Internetga kirish huquqini olish uchun murojaat qilish;
- Internetdan foydalanish huquqiga to‘sqinlik qiladigan texnik xatolar bo‘lsa, administrator bilan bog‘lanish;
- Internetga kirishda kontentni filtrlash qoidalarini o‘zgartirish bo‘yicha takliflar kiritish;

- shaxsiy kompyuter texnikasini ajratish va modernizatsiya qilish hamda foydalanish uchun zarur bo‘lgan dasturiy ta’minotni o‘rnatish uchun arizalar taqdim etish.

Internet orqali ma’lumot olish va tarqatish

1. Jamiyat xodimlari o‘zlarining ish joylaridan internetga kirish imkoniyatiga ega bo‘ladilar. Xodimlar ma’lumotni qabul qilish va tarqatish uchun Internetga kirish huquqiga ega.

2. Jamiyat xodimlari internetdan o‘zlarining ish faoliyatiga oid vazifalarini bajarish uchun zarur bo‘lgan har qanday ma’lumotni qidiruv tizimlari orqali internetdagi axborot resurslariga kirish yoki URL manzilini kiritish orqali olishlari mumkin.

3. Jamiyat xodimlari internetda quyidagilarni amalga oshirishi mumkin:

- Jamiyat va uning bo‘linmalari faoliyati to‘g‘risida jamoatchilikka ma’lum bo‘lgan ma’lumotlarni olish;
- Jamiyatning ommaviy tadbirlari to‘g‘risidagi yangiliklar va axborotlarni tarqatish;
- Jamiyat bilan o‘zaro aloqada bo‘lgan uchinchi tomon tashkilotlari uchun zarur bo‘lgan ma’lumotlarni yetkazib berish;
- Jamiyat bilan o‘zaro aloqada bo‘lish uchun ochiq aloqa ma’lumotlarini va boshqa ma’lumotlarni taqdim etish.

4. Yuqoridagi ma’lumotlarni tarqatish huquqi Jamiyat xodimlariga o‘zlarining xizmat vazifalariga muvofiq ravishda va faqat Jamiyat rahbariyatidan bunday tarkibni tarqatish zarurligi to‘g‘risida olingan topshiriqning bajarilishi munosabati bilan beriladi.

5. Jamiyatning internetga ulanish huquqiga ega bo‘lgan xodimlarining ro‘yxatini shakllantirishda, uning internetda ma’lumot olish va tarqatish bo‘yicha huquq va majburiyatlari ko‘rsatiladi.

6. Jamiyatning internetga ulanadigan xodimlar ro‘yxati uning bevosita rahbari va bo‘lim boshliqlari tomonidan tasdiqlangan yoki iltimosiga binoan shakllantiriladi. Ko‘rsatilgan arizada internetdan foydalanish zarurati, foydalanuvchilarning huquqlari va majburiyatlari ko‘rsatilishi kerak.

7. Internetga ma’lumot tarqatishda Jamiyat xodimlari quyidagi talablarga rioya qilishlari shart:

- ishonchli, to‘liq va obyektiv ma’lumotlarni nashr etish;
- materiallarni nashr etishda, shu jumladan shaxsiy fikrlarini bildirganda, faqat o‘zlarining ish faoliyatiga oid vazifalariga tayanishlari;
- nashr etilgan materiallar uchun to‘liq javobgarlikni anglash;
- intellektual faoliyat natijalari va individualizatsiya vositalariga nisbatan uchinchi shaxslarning huquqlarini kuzatish va hurmat qilish;
- boshqa internet foydalanuvchilari bilan to‘qnashuvlar va nizolardan saqlanish.

8. Quyidagi ma’lumotlarni o‘z ichiga olgan materiallarni nashr etish, yuklab olish va tarqatish taqiqlanadi:

- konfidensial ma’lumotlar, shuningdek tijorat sirini tashkil etuvchi ma’lumotlar, agar u xizmat vazifalariga kirmasa va uzatish usuli xavfsiz bo‘lsa,

(Raqamlashtirish boshqarmasi) lokal tarmoq administratori bilan oldindan kelishib olinmagan bo‘lsa;

- egasining ruxsatisiz, to‘liq yoki qisman mualliflik huquqi yoki boshqa huquqlar bilan himoyalangan ma’lumotlar;

- ruxsatsiz kirish uchun har qanday apparat va dasturiy ta’minotni buzish, yo‘q qilish yoki cheklash uchun mo‘ljallangan zararli dastur, shuningdek tijorat dasturlari va ularni ishlab chiqarish uchun dasturiy ta’minot uchun seriya raqamlari, parol va pullik internetga ruxsatsiz kirish huquqini beradigan boshqa vositalar;

- tahdid soluvchi, tuhmat, noma’qul ma’lumot, shuningdek boshqalarning sha’ni va qadr-qimmatini kamsituvchi ma’lumotlar, etnik nafratni qo‘zg‘atuvchi, zo‘ravonlikni qo‘zg‘atuvchi, noqonuniy xatti-harakatlarni sodir etishga chaqiruvchi materiallar va boshqalar;

- IP-manzilini va boshqa xizmat ma’lumotlarini qalbakilashtirish.

9. Internetdan yuklab olingan barcha fayllar zararli dasturlarning mavjudligi bo‘yicha majburiy ravishda tekshirilishi shart.

10. Quyidagilar taqiqlanadi:

- tarmoq yukini oshiradigan va boshqa foydalanuvchilarning normal ishlashiga xalaqit beradigan video oqimlarning uzatiladigan manbalardan foydalanish;

- shubhali hisoblangan internet resurslariga (pornografiya, milliy yoki diniy nafrat, xaqorat, tahdid, zo‘ravonlikni, millatchilikni va terrorizmni targ‘ib etuvchi manbalar) kirish va ulardan foydalanish;

- internetda noqonuniy operatsiyalarni amalga oshirish va qonun hujjatlariga, shuningdek ushbu qo‘llanmaga zid bo‘lgan boshqa harakatlarni bajarish.

11. Axborot va kiberxavfsizlik bo‘limi xodimlari xodimlarning axborot xavfsizligi siyosatiga zid bo‘lgan ba’zi bir internet-resurslaridan foydalanishni tarmoqlararo ekran va proksi-server orqali cheklash huquqiga ega.

Internet-resurslardan foydalanish bo‘yicha nazorat

1 Jamiyat xizmat majburiyatlarini bajarish bilan bog‘liq bo‘lmagan internet-resurslarni, shuningdek, mazmuni va yo‘nalishi xalqaro va milliy qonun hujjatlarida taqiqlangan manbalarga kirishni cheklash huquqini o‘zida saqlab qoladi.

2. Jamiyat markaziy apparat (Raqamlashtirish boshqarmasi) lokal tarmoq administratorlari xodimlar tomonidan internet-resurslardan foydalanish hisobini yuritadilar, ushbu yo‘riqnomaga rioya qilinishini nazorat qiladilar va internet-resurslardan xavfsiz foydalanilishni ta’minlaydilar.

3. Axborot va kiberxavfsizlik bo‘limi xodimlari Jamiyat xodimlarining internet tarmog‘idan maqsadli foydalanilishini tanlab yoki to‘liq oldindan kelishilmagan holda, shuningdek onlayn tekshirishni amalga oshirish huquqiga ega.

4. Xodimlar tashrif buyurgan internet-manbalar to‘g‘risidagi ma’lumotlar keyinchalik tahlil qilish uchun qayd qilinadi va zarur bo‘lganda ularni monitoring qilish uchun tarkibiy bo‘linmalar rahbarlariga, shuningdek Jamiyat rahbariyatiga taqdim etish mumkin. Jamiyatning barcha xodimlari internetga va/yoki ularga taqdim etilgan axborot kommunikatsiya vositalaridan faqat ishlab chiqarish ehtiyojlari uchun foydalanishlari shart.

5. Internet foydalanuvchilarning faoliyatini kuzatadigan maxsus dasturiy ta'minot ishining natijalariga, shuningdek internetdan maqsadli foydalanishda qisman va to'liq tekshiruv natijalariga ko'ra eng zararli buzuvchilari aniqlandi.

6. Noto'g'ri foydalanish holatlari (Raqamlashtirish boshqarmasi) lokal tarmoq administratorlari tomonidan Axborot xavfsizligi administratori ishtirokida "Internetdan noto'g'ri foydalanish to'g'risidagi bayonnoma" ko'rinishida qayd etiladi.

Aniqlangan internetni suiste'mol qilish faktiga ko'ra, qoidabuzardan tushuntirish xati ko'rinishidagi yozma ariza olinadi.

Internet tarmog'idan noto'g'ri foydalanish to'g'risidagi bayonnoma Axborot va kiberxavfsizlik bo'limi boshlig'i hisoboti bilan tasdiqlanadi va Jamiyat yoki uning tizim korxona rahbariga qaror qabul qilish uchun taqdim etiladi.

7. Agar xodim internetdan noto'g'ri foydalanishda gumon qilinsa, ichki audit o'tkaziladi.

Korporativ elektron pochtadan foydalanish qoidalari

1. Korporativ elektron pochta bilan ishlashda foydalanuvchi quyidagilarni hisobga olishi kerak:

- Elektron pochta - bu yuborilgan xabarni qabul qiluvchiga kafolatli yetkazish vositasi emas;

- Elektron pochta - bu uzatilayotgan ma'lumotlarning konfidensialligini ta'minlaydigan ma'lumotni uzatish vositasi emas. Konfidensial ma'lumotlarni uzatishga faqat xavfsiz ulanishlar yoki E-xat elektron pochta tizimi orqali ulanish mumkin.

2. (Raqamlashtirish boshqarmasi) lokal tarmoq administratori foydalanuvchining pochta qutisi va uzatiladigan ma'lumotlar umumiy hajmiga elektron pochta serverini tashkil qilish uchun ishlatiladigan dasturiy ta'minot va telekommunikatsiya va server uskunalarining hozirgi imkoniyatlaridan kelib chiqib cheklov qo'yadi. Saqlangan yoki uzatiladigan ma'lumotlar belgilangan chegaradan oshib ketgan taqdirda, pochtaga kirish bloklanadi. Pochtaga kirish bloklangan bo'lsa, uning pochta qutisi hajmi oshib ketishi va foydalanuvchi pochta qutisini tozalash zarurligi to'g'risida xabar paydo bo'ladi.

3. Korporativ elektron pochta foydalanuvchilariga quyidagilar taqiqlanadi:

- korporativ elektron pochtadan har qanday shaxsiy yozishmalar yoki tijorat maqsadlarida foydalanish;

- siyosiy, diniy, insoniylikka qarshi xarakterdagi, shuningdek, odobsiz, tuhmat, haqoratli, tahdid soluvchi yoki noqonuniy materiallarni korporativ elektron pochta yoki boshqa elektron vositalar orqali yuborish, saqlash va foydalanish. Shunga o'xshash xarakterga ega ma'lumotlar paydo bo'lganda, foydalanuvchi darhol o'zining bevosita rahbarini xabardor qilishi shart.

- reklama (sohaga oid bo'lmagan) va ko'ngilochar xarakterdagi materiallarni yuborish;

- ish faoliyatiga aloqasi bo'lmagan xatlarning ommaviy tarqatilishini amalga oshirish;

- zararli dasturlarni yoki viruslarni yuqtirgan fayllarni yuborish;

- rasmiy yozishmalar uchun bepul internet pochta xizmatlaridan (mail.ru, yandex.ru va boshqalar) foydalanish;

- uchinchi shaxsga o‘z pochta qutilariga kirish uchun parolini berish;

4. Uzatilgan elektron pochta xabari va boshqa elektron hujjatlarning mazmuni aniq, qisqa va tushunarli bo‘lishi kerak.

5. Quyidagilar qattiq taqiqlangan:

- yozishmalar va rasmiy ma’lumot almashish uchun .UZ domen zonasidan tashqarida ruxsatsiz tashqi pochta xizmatlaridan foydalanish;

- Konfidensial ma’lumotni himoyalanmagan shaklda elektron pochta orqali yuborish.

1.3. Parol bilan himoya qilish bo‘yicha yo‘riqnoma

1. Umumiy xolat

1.1 Ushbu yo‘riqnoma Jamiyatning axborotlashtirish vositalariga kirishda xodimlarning parol bilan himoyalanishi va autentifikatsiyasiga qo‘yiladigan talablarni, qoidalarini va ishlatish tartibini belgilaydi.

1.2 Ushbu yo‘riqnoma parol bilan himoya qilishni va axborotlashtirish obyektlariga kirishning boshqa identifikatorlarini shakllantirish, boshqarish, shuningdek ushbu obyektlarga kirish huquqiga ega bo‘lgan barcha xodimlarga nisbatan qo‘llaniladi.

1.3 Ushbu yo‘riqnoma parollarni himoya qilish vositalarini yaratuvchi va boshqaradigan xodimlarga va parol bilan himoyadan foydalangan holda Jamiyat markaziy apparati va tizim tashkilotlariga tegishli.

1.4 Jamiyat xodimlarining parollari konfidensial ma’lumotlar bo‘lib, ularni komprometatsiyaga uchrashi yoki birovga berish mumkin emas. Parol xavfsizligini ta’minlash uchun egasi javobgardir.

2. Parollarni xavfsiz saqlashga qo‘yilgan talablar

2.1 Shaxsiy parolini sir saqlash uchun foydalanuvchi shaxsan javobgardir. Parol komprometatsiyasi, shuningdek parolni jamoat joylarida saqlash taqiqlanadi.

2.2 Xodim o‘z parollarini qog‘ozda saqlashga faqat parol egasi tomonidan shaxsiy muhr bilan muhrlangan qutida yoki bo‘linma boshlig‘i seyfida saqlashga ruxsat etiladi.

2.3 Zarurati tug‘ilganda (xizmat safari, ta’til va boshqalar), Axborot va kiberxavfsizlik bo‘limi tomonidan amalga oshiriladigan tekshirish faoliyatini amalga oshirishda foydalanuvchi parolini talab qiladigan bo‘lsa, uning parolini komprometatsiya qilishga ruxsat beriladi.

2.4 Parolni berish faktini foydalanuvchi tomonidan Axborot va kiberxavfsizlik bo‘limi boshlig‘iga yetkazish kerak. Ishlab chiqarish yoki tekshirish ishlarining oxirida foydalanuvchilar mustaqil ravishda “komprometatsiyaga uchragan” parollarni darhol majburiy ravishda o‘zgartirishlari shart.

2.5 Favqulodda vaziyatlar, shuningdek foydalanuvchi qayd yozuvi va parollarni o‘zgartirishga texnologik ehtiyoji tug‘ilgan taqdirda axborot xavfsizligi administratoriga parollarni o‘zgartirishga ruxsat beriladi. Bunday hollarda parollari o‘zgartirilgan foydalanuvchilar o‘zlarining parollari o‘zgartirilganligini bilgandan so‘ng darhol yangi parol yaratishga majburdirlar.

2.6 Agar foydalanuvchi uzoq vaqt ishda bo‘lmagan taqdirda (xizmat safari, kasallik va boshqalar), uning akkaunti bloklanadi, zarur hollarda ushbu foydalanuvchi resurslariga nisbatan boshqa foydalanuvchilarning kirish huquqlari o‘zgartiriladi. Axborot xavfsizligi administratoriga foydalanuvchi uzoq vaqt davomida yo‘qligi to‘g‘risida xabar berilishi kerak.

2.7 Parol egalari yuqorida sanab o‘tilgan talablardan xabardor bo‘lishlari va ushbu talablarga javob bermaydigan parollardan foydalanish, shuningdek parol ma’lumotlarini oshkor qilish mas’uliyati haqida ogohlantirishlari lozim.

3. Parol yaratish jarayonlarini tashkiliy va texnik jihatdan ta’minlash

3.1 Jamiyatda ishga yangi qabul qilingan xodimlar uchun ishchi stansiyalar, lokal tarmoq va elektron pochta xizmatlaridan foydalanish, shuningdek axborot resurslariga kirish uchun yangi foydalanuvchi qayd yozuvi va ishga tushirish parollari yaratiladi.

3.2 Lokal tarmoq hamda elektron pochta xizmatidan foydalanish uchun yangi foydalanuvchi qayd yozuvi va boshlang‘ich parollar axborot xavfsizligi administratori yoki lokal tarmoq administratori tomonidan yaratiladi domen serveriga kiritiladi.

3.3 Initsializatsiya qilingan parolni ishlab chiqarishda ushbu qo‘llanmaning 5-bo‘limida belgilangan parollarni ishlab chiqarish talablari va qoidalari bajarilishi kerak.

3.4 Ishchi stansiyalariga kirish uchun boshlang‘ich parol yangi xodimga korporativ elektron pochta orqali yoki shaxsan o‘ziga taqdim etiladi.

4. Parollarni o‘zgartirish va bekor qilish jarayoni

4.1 Parol shakllangandan so‘ng, yangi xodim ushbu yo‘riqnomaning 5-bo‘limida belgilangan parollarni ishlab chiqarish talablari va qoidalariga rioya qilgan holda o‘z parolini kiritishi shart.

4.2 Jamiyat xodimlari ishchi stansiyalari va lokal tarmoqqa kirishdagi parollarni 3 oyda bir marotaba o‘zgartirishlari kerak.

4.3 Vakolatsiz shaxslarning serverga, tarmoq uskunalariga va axborotni muhofaza qilish vositalariga kirishini cheklash, ularga kirish parollari, shuningdek ularga masofadan kirishni ta’minlaydigan ishchi stansiyalari, ularning ishlashi uchun mas’ul xodimlar - axborot xavfsizligi administratori va mintaqaviy administratorlari tomonidan shakllantiriladi va foydalaniladi.

Belgilangan parollar rejaga asosan o‘zgartirish (Axborot va kiberxavfsizlik bo‘limi) axborot xavfsizligi administratori tomonidan har 3 oyda bir marta amalga oshirilishi kerak.

4.4 Jamiyat xodimlarining axborot resurslariga kirishi parol asosida amalga oshiriladi, uning rejadagi o‘zgarishi Jamiyat xodimlari tomonidan 3 oy ichida kamida bir marta amalga oshiriladi. Bu talab nazorat tizimini tartibga solish va axborot resurslariga kirishni nazorat qilish bilan ta’minlanishi lozim.

4.5 Agar parol kompрometatsiyaga uchragan deb gumon qilingan bo‘lsa, Jamiyat xodimi darhol axborot xavfsizligi administratoriga (Axborot va kiberxavfsizlik bo‘limi) xabar berishi shart. Javobgar xodimlar esa darhol

foydalanuvchini qayd yozuvini blokirovka qilishi va parolni rejadan tashqari o‘zgartirishi kerak.

4.6 Xodimning qayd yozuvlarini o‘chirish orqali kirishni blokirovka qilish uning vakolatlari tugatilgan taqdirda (ishdan bo‘shatish, boshqa ishga o‘tish va h.k.) amalga oshiriladi va ushbu xodimning tizimdagi so‘nggi sessiyasi tugagandan so‘ng darhol amalga oshirilishi kerak.

4.7 Barcha foydalanuvchilar uchun parollarning rejadan tashqari to‘liq o‘zgarishi administrator va parol himoyasini boshqarish vakolatiga ega bo‘lgan boshqa xodimlar tomonidan amalga oshirilishi kerak.

Ishchi stansiyalari va serverlar, agar foydalanuvchi 10 daqiqa ishchi holatida bo‘lmasa blok holatiga, 60 daqiqa uxlash rejimiga va 120 daqiqada kutish holatiga o‘tishi avtomatlashtirilgan tarzda bo‘lishi kerak.

5. Parollarni yaratish uchun talablar

5.1 Jamiyatning axborotlashtirish obyektlariga kirish uchun parollarni shakllantirishda quyidagi talablarga javob berish kerak:

- parolning minimal uzunligi kamida 8 ta belgiladan iborat bo‘lishi kerak;
- parol belgilarida katta va kichik harflar, raqamlar va maxsus belgilardan iborat bo‘lishi kerak;
- parolda oson hisoblanadigan belgilar kombinatsiyalari (ismlar, familiyalar, tug‘ilgan kunlar va boshqalar), shuningdek, umumiy qabul qilingan qisqartmalardan (LAN, USER va boshqalar) iborat bo‘lmasligi kerak;
- parolni o‘zgartirganda, yangi qiymat kamida 6 holatda avvalgisidan farq qilishi lozim.

5.2 Axborot xavfsizligi va lokal tarmoq administratorlarining paroli kichik va katta harflar, raqamlar va maxsus belgilar yordamida kamida 12 ta belgi bo‘lishi kerak.

5.3 Parollarni generatsiyalash va tarqatish jarayonlari lokal tarmoq administratori tomonidan amalga oshiriladi. Ushbu vazifalar Axborot va kiberxavfsizlik bo‘limi boshlig‘i tomonidan nazorat qilinadi.

6. Parollar bilan ishlashda xodimlar va mas’ul xodimlarining harakatlarini nazorat qilish

6.1 Parollar bilan ishlashda xodimlar va mas’ul xodimlarning harakatlari ustidan nazorat qilish axborot xavfsizligi administratorlariga, hududiy boshqarmalarda esa – mintaqaviy axborot xavfsizligi administratorlarga yuklatilishi lozim.

6.2 Parollar bilan ishlashda xodimlar va lokal tarmoq administratorining harakatlari ustidan tashkiliy va texnik nazorat Bo‘lim boshlig‘i tomonidan har 6 oyda bir marta amalga oshiriladi.

6.3 Parollar bilan ishlashda xodimlar harakatlari ustidan nazorat quyidagilar asosida amalga oshiriladi:

- ushbu yo‘riqnomaga muvofiq parollarni saqlash talablari;
- ushbu yo‘riqnomaning 9-bo‘limiga muvofiq parol egalarining majburiyatlari.

Foydalanuvchilarning parollarining xavfsizligini ta’minlash uchun tasodifiy tekshirish (so‘rov, so‘rovnoma, tekshirish) amalga oshiriladi.

Axborot xavfsizligi administratori foydalanuvchilar tomonidan kiritgan parolning murakkabligi va saqlanish holatini tekshiradi.

6.4 Ushbu yo‘riqnoma talablari buzilgan taqdirda axborot xavfsizligi administratori takroran buzilishning oldini olish maqsadida foydalanuvchilarga ogohlantirish berishi shart.

Xodim tomonidan ushbu ko‘rsatma talablari muntazam yoki qo‘pol ravishda buzilgan taqdirda, lokal tarmoq administratori buzg‘unchiga nisbatan tegishli choralar ko‘rish uchun Bo‘lim boshlig‘ini xabardor qilishi kerak.

7. Vazifalari va majburiyatlari

7.1 Jamiyat xodimlari quyidagilarga majbur:

- turli axborotlashtirish obyektlariga kirishda har bir qayd yozuvlari uchun turli parollarni qo‘llash;
- axborot xavfsizligi administratoriga kirishni blokirovka qilish uchun ularning paroli buzilganligi to‘g‘risida xabar berish;
- parol xavfsizligini ta’minlash;
- begona shaxslarga va xodimlarga shaxsiy parolni oshkor qilmaslik.

7.2 Jamiyat xodimlari o‘z parollarini himoya qilish bo‘yicha yetarli choralarni qo‘llashlari shart, shu jumladan:

- shaxsiy parolni yodda saqlash va boshqa xodimlarni bilmasligini taminlash;
- shaxsiy parolni faqatgina tarkibiy bo‘linma raxbaridan tashqari har qanday vaziyatda xech kimga bermaslik;
- paroldan foydalanganda (masalan, uni kiritish), uning buzilish ehtimolini istisno qilish uchun zarur choralarni ko‘rish (masalan, kiritilgan parolni vizual ko‘rish imkoniyatini istisno qilish).

7.3 Xodim tomonidan ishlatilgan parollardan Jamiyatdan tashqaridagi tizimlarda (masalan, internet-saytlarda, internet-do‘konlarda, elektron to‘lov tizimlarida va boshqalarda) foydalanish taqiqlanadi.

7.4 Axborot xavfsizligi administratoriga xodimlarning parollarini aniq matnda yoki xesh qiymatlari shaklida saqlash, shuningdek parollarni umumiy resurslarga joylashtirish yoki elektron pochta orqali yuborish taqiqlanadi (parollarni faqat korporativ elektron pochta orqali xodimning o‘ziga yuborishdan tashqari).

7.5 Lokal tarmoq administratorining parollarni saqlash majburiyatlari:

- xodimlarni parollarni himoya qilish, parollarning xavfsizligini ta’minlash va parolni buzish uchun javobgar bo‘lish to‘g‘risida ogohlatirish;
- Jamiyat xodimlarining parollari buzilgan taqdirda Bo‘lim boshlig‘iga zudlik bilan xabar berish.

1.4. Foydalanish uchun ruxsat etilgan dasturiy ta’minot ro‘yxati

1. Jamiyat markaziy apparat va uning korxonalarida operatsion tizim va uning tarkibiy qismlarini, ishchi stansiyalari bo‘yicha dasturiy ta’minotni o‘rnatish va yangilash (Raqamlashtirish boshqarmasi) lokal tarmoq administratorlari tomonidan amalga oshiriladi. Xodimlarga ishchi stansiyalarda operatsion tizim, dasturiy ta’minotlarni mustaqil ravishda o‘rnatishga yo‘l qo‘yilmaydi.

2. Jamiyat xodimlarining ishchi stansiyalarida o‘rnatilishi ruxsat etilgan dasturiy ta’minotlar ro‘yxati 1-jadvalga muvofiq, Jamiyat serverlariga o‘rnatilgan dasturlar ro‘yxati 2-jadvalga muvofiq keltirilgan.

3. Ma’lum bir vazifani bajarishga ixtisoslashgan ishchi stansiyalari uchun barcha istisnolar Axborot va kiberxavfsizlik bo‘limi yoki Raqamlashtirish boshqarmasi bilan yozma ravishda kelishilishi va Jamiyat rahbariyati tomonidan tegishli buyruq orqali rasmiylashtirilishi kerak.

4. Axborot va kiberxavfsizlik bo‘limi Jamiyat rahbariyati bilan kelishgan holda boshqa shunga o‘xshash dasturiy ta’minotni ishlab chiqaruvchilar tomonidan yangilanishlar chiqarilishini to‘xtatgan, shuningdek funksional jihatdan ustun bo‘lgan yoki ro‘yxatda ko‘rsatilganlardan pastroq narxga ega bo‘lgan yangi dasturlarning paydo bo‘lganda foydalanishga ruxsat berish huquqiga ega.

5. Jamiyat xodimlariga ishchi stansiyalar foydalanuvchi huquqlari bilan beriladi.

1-jadval

Jamiyat xodimlarining ishchi stansiyalarida o‘rnatilishi ruxsat etilgan dasturiy ta’minotlar ro‘yxati

№	Dastur tavsifi	Dasturiy mahsulot nomi	Dasturiy mahsulot ishlab chiqaruvchisi	Litsenziya amal qilish muddati *	Versiyasi va sborkasi*
1.	Operatsion tizimlar	Windows 7	Microsoft Corporation		Professional 64/32
		Windows 10			Professional 64/32
		Windows 11			Professional
		Linux	ochiq kodli		Ubuntu 18.04/20.04/22.04
		MacOS	Apple		
2.	Virusdan himoyalovchi dastur	ESET Endpoint Security	ESET		10.1.2046 11.1.2052
		Kaspersky Endpoint Security	Kaspersky		
3.	Ofis dasturlari	MS Office	Microsoft Corporation		2003/2007/2010/2016/2019/2021/2024
		MS Word uchun Savodxon	Savodxon loyihasi		
4.	Arxivlovchi dasturlar	7-Zip	RARLAB		
		WinRar			

5.	Internet brauzerlar	Internet Exploler	Microsoft Corporation		
		Mozilla Firefox	Mozilla		
		Chrome	Google		
		Safari	Apple		
6.	Elektron pochta	E-xat	Unicon uz		
		Outlook	Microsoft		
		Zimbra	Ochiq kodli		
		Webmail	Roundcube Webmail		
7.	PDF fayllarni ko‘ruvchi dasturlar	Adobe Acrobat reader,	Adobe Systems Incorporated		
		ABBYY FineReader	ABBYY Production LLC		
		Foxit Reader			
		PDF 24 Creator	Geek software GmbH		
8.	Video player	Windows Media Player	Microsoft Corporation		
		K-Lite Codec Pack	Codec Guide		
		Pot player			
9.	Audioplayer	AIMP	Ochiq kodli AIMP		
10.	Fayl menedjeri	Total commander	Ochiq kodli GNU GPL		
11.	Masofaviy boshqarish	RDP	Microsoft		
		TeamViewer	TeamViewer AG		
		AmmyyAdmin			
		AnyDesk	AnyDesk Software GmbH		

		Radmin	Radmin		
12.	Elektron imzo uchun	E-IMZO	Unicon		
13.	Buxgalter hisoboti va tahlili uchun dastur	1C	1C Company		8.3.10.2252
		eStat	stat.uz		
		Norma Hamkor	Norma		
14.	Video konferensiya dasturi	Zoom Workplace	Zoom Video Communications Inc.		
		Cisco Jabber	Cisco		
		Teams	Microsoft		
		Telemetriya	Yandex		
		Meet	Google		
		TrueConf	TrueConf		
15.	Grafik dasturlar	Photoshop	Adobe Systems		
		Corel DRAW			
		Adobe Illustrator	Adobe Systems		
		Adobe After Effects	Adobe Systems		
		AutoCAD	Autodesk		
16.	Video Kuzatuv dasturlar	Ivms 4200	Hikvision		
17.	Wireshark analiz trafik	Wireshark	Wireshark		
18.	Putty komutatorlarga masafodan bog‘lanish uchun	Putty	Putty		
19.	SIEM dasturilari	Wazuh	ochiq kodli		
20.	DLP				

21.	HRM				
22.	EDO ijro				

**Izoh: Dasturlar versiyasi va sborkasi Kompyuter tizimi administratori tomonidan doimiy yangilab borilganligi bois qo'lda to'ldirib boriladi.*

2-jadval

Jamiyat serverlariga o'rnatilgan dasturiy ta'minotlar ro'yxati

№	Dastur tavsifi	Dasturiy mahsulot nomi	Dasturiy mahsulot ishlab chiqaruvchisi	Litsenziya amal qilish muddati*	Versiyasi va sborkasi*
1.	Server operatsion tizimlar	Microsoft Windows Server	Microsoft Corporation inc		2003/2006/2009/2016/2019/2022
		linux-debian	ochiq kodli		
2.	Internet - trafikni tarqatish dasturi (proksi - server)	Web Proxy & Filter (NethServer)	ochiq kodli		1.14.2
		-	-		
3.	Virusdan himoyalovchi dastur	Eset Endpoint Security	ESET		10.1.2046
4.	Ochiq kodli virtualizatsiya tizimi	ESXI	VMware		
5.	Telefon tizimi				
6.	WebMail (WebTop)	WebMail (NethServer)	ochiq kodli		1.8.21
7.	Windows xp,	Windows xp,	Microsoft		7/10
8.	Ubunto debian	Linux	Linux		16.04/22.04
9.	IP Telefon	Grandstream	Grandstream		

10.	Shifirlangan VPN lokal tarmoq uchun	Kerio Winroute Firewall	Kerio Winroute Firewall		
		Open VPN (NethServer)	Open VPN (NethServer)		

1.5 Antivirus himoyasi bo‘yicha yo‘riqnoma

Umumiy qoidalar

1. Ushbu yo‘riqnoma axborotni va Jamiyat axborot-kommunikatsiya tizimini zararli dasturlarning xatti-harakatlaridan himoya qilishni ta’minlashni tashkil etish tartibi va talablarini belgilaydi.

2. Ushbu yo‘riqnoma axborot-kommunikatsiya tizimidan foydalanganda markaziy apparatning va Jamiyat hududiy filiallarining barcha xodimlari uchun majburiydir.

Antivirusdan himoya qilish ishlarining ishtirokchilariga qo‘yiladigan talablar

3. Ishchi stansiyalari va serverlarini o‘rnatilgan antivirus dasturisiz ishlatish taqiqlanadi. Antivirus dasturini doimiy yangilab turish kerak.

4. Agar zararli dastur mavjudligiga shubha tug‘ilsa (dasturlarning noto‘g‘ri ishlashi, grafik va ovoz effektlarining paydo bo‘lishi, ma’lumotlarning buzilishi, yo‘qolgan fayllar, tizim xatosi haqidagi xabarlarning tez-tez paydo bo‘lishi), foydalanuvchining o‘zi yoki (Axborot va kiberxavfsizlik bo‘limi) axborot xavfsizligi administratori bilan birgalikda o‘z ishchi stantsiyasida antivirus nazoratini amalga oshirishi kerak.

5. Kompyuter viruslarini yuqtirgan fayllarni antivirus tekshiruvi paytida aniqlangan bo‘lsa, foydalanuvchilar:

- ishni to‘xtatib qo‘yish;
- virusni yuqtirgan fayllar aniqlanganligi to‘g‘risida (Axborot va kiberxavfsizlik bo‘limi) axborot xavfsizligi administratorini shuningdek ushbu fayllardan o‘z ishlarida foydalanadigan foydalanuvchilarni darhol xabardor qilish kerak;
- undan keyingi foydalanish tahlilini o‘tkazish;
- zararlangan fayllarni zararsizlantirish yoki yo‘q qilish;
- agar antivirus dasturi zararsizlantira olmagan yangi virus aniqlansa, virus bilan zararlangan faylni (Axborot va kiberxavfsizlik bo‘limi) axborot xavfsizligi administratoriga taqdim etish kerak.

6. Xodimlarga ishchi stansiyasidan axborot xavfsizligi administratorining (Axborot va kiberxavfsizlik bo‘limi) roziligisiz quyidagilar taqiqlanadi:

- antivirus himoya vositalari sozlamalari va konfiguratsiyasini o‘zgartirish;
- virusga qarshi himoya vositalarini olib tashlash yoki tizimga qo‘shish;
- ishchi stansiyasida o‘rnatilgan antivirus himoyasi vositalarini tekshirmasdan turib saqlash vositalaridan foydalanish;
- elektron pochta orqali kelgan noma’lum dasturlarni ishga tushirish.

7. Foydalanuvchilar quyidagilarga majbur:

- noma'lum, shubhali yoki ishonchsiz manbalardan olingan elektron pochta xabarlariga qo'shimchalarni ochmaslikga. Bunday biriktirilgan fayllar tezda o'chirilishi kerak;
- noma'lum yoki shubhali manbalardan ma'lumotlarni yuklamaslik;
- mantiqiy disklarga kirishni bekor qilish;
- noma'lum yoki shubhali manbalardan olingan axborot tashuvchisidan foydalanishdan oldin, uni viruslardan tekshirish;
- har kuni, ishchi stansiyasini dastlabki yuklashda, rezident antivirus monitor mavjudligiga ishonch hosil qilish va agar mavjud bo'lmasa, axborot xavfsizligi administratorini xabardor qilish;
- Axborot xavfsizligi administratoridan tizimda virus mavjudligi to'g'risida, shuningdek, virusga shubha tug'ilganda xabarnoma olingandan so'ng, ishchi stansiyasini rejadan tashqari antivirus tekshiruvini mustaqil ravishda amalga oshirish.

1.6 Mobil, ma'lumot saqlovchi va tashuvchi qurilmalar bilan ishlashda axborot xavfsizligini ta'minlash bo'yicha yo'riqnoma

1. Ushbu yo'riqnoma Jamiyatda foydalaniladigan axborot tashuvchi vositalar, mobil qurilmalar, ma'lumotlarni saqlash moslamalari bilan ishlashda axborot xavfsizligini ta'minlash talablari va tartiblarini belgilaydi.

2. Axborot-kommunikatsiya tizimlarida, ish stansiyalari va lokal tarmoqda ma'lumotlarni qayta ishlash, qabul qilish, uzatish maqsadida mobil qurilmalar va qo'shimcha ma'lumotlarni saqlovchi va tashuvchi tashqi qurilmalar foydalanishni anglatadi.

3. Foydalaniladigan axborot tashuvchi vositalar, mobil qurilmalar sifatida USB flesh-xotiralar, qattiq disklar va noutbuklardan (keyingi o'rinlarda - mobil qurilmalar) foydalaniladi.

Qo'llash qoidalari va talablar

4. Jamiyat xodimlarga tegishli bo'lgan tashuvchi, saqlovchi va mobil qurilmalar foydalanish quyidagi hollarda taqiqlanadi:

- konfidensial muzokaralar va konfidensial xarakterdagi tadbirlar o'tkaziladigan xonalarda;
- lokal tarmoq va axborot tizimlariga ulanish uchun;
- masofadan foydalanuvchilarning mobil qurilmalarini umumiy foydalanishdagi telekommunikatsiya tarmog'i va internet orqali axborot tizimiga va lokal tarmoqqa ulash;
- konfidensial yoki boshqa himoyalangan ma'lumotlarni, shu jumladan parollarni va boshqalarni tashuvchilar sifatida foydalanish.

5. Axborot-kommunikatsiya tizimida faqat Jamiyatning mulki bo'lgan va ro'yxatdan o'tgan mobil qurilmalar, ma'lumotlarni saqlovchi va tashuvchi tashqi qurilmalardan foydalanishga ruxsat beriladi.

6. Mobil qurilmalaridan faqat Jamiyat axborot tizimlariga ulanish uchun faqat boshqariladigan hudud doirasida foydalanish mumkin. Bunday holda, ularga qo'yiladigan talablar ish stansiyalari bilan bir xil.

7. Mobil qurilmalar va ma'lumotlarni saqlovchi va tashuvchi tashqi qurilmalardan foydalanish paytida, Jamiyat xodimlari quyidagi talablarni bajarishlari kerak:

- ulardan belgilangan maqsadlarda va faqat xizmat vazifalarini bajarishda foydalanish;
- lokal tarmoq administratoriga ushbu Yo'riqnomaning talablari buzilganligi to'g'risida xabar berish;
- lokal tarmoq administratoriga mobil qurilmalar, ma'lumotlarni saqlovchi va tashuvchi tashqi qurilmalarning yo'qolishi (o'g'irlanishi) to'g'risida xabar berish;
- mobil qurilmalar, ma'lumotlarni saqlovchi va tashuvchi tashqi qurilmalarni jismoniy xavfsizligini har qanday oqilona usulda ta'minlash;
- mobil qurilmalar va ma'lumotlarni saqlovchi va tashuvchi tashqi qurilmalarni boshqa shaxslarga bermaslik.

8. Hisobga olingan mobil qurilmalar, ma'lumotlarni saqlovchi va tashuvchi tashqi qurilmalar Jamiyat xodimlari tomonidan qarovsiz qoldirilishi taqiqlanadi.

9. Jamiyatdan tashqarida (xizmat safarlari, uchrashuvlar, muzokaralar va boshqalar) ishlatilganda mobil qurilmalarning axborot va jismoniy xavfsizligini ta'minlash uchun quyidagi choralar qo'llanilishi kerak:

- mobil qurilmaga kirishda foydalanuvchi biometrik ma'lumotlari asosida kirish parolini o'rnatish yoki autentifikatsiya vositalaridan foydalanish;
- mobil qurilmaning ma'lum dasturlariga kirish uchun parolni o'rnatish;
- mobil qurilmada virusga qarshi himoya va shaxsiy tarmoqlararo ekranidan foydalanish.

Vositalaridan foydalanish qoidalari va talablari

10. Jamiyat axborot infratuzilmasida faqat Jamiyatning mulki bo'lgan va nazoratga olinadigan, ro'yxatdan o'tgan axborot tashuvchi vositalaridan foydalanishga ruxsat beriladi.

11. Axborot tashuvchi vositalar vaqti-vaqti bilan haftasiga kamida bir marta virusga qarshi dasturlar yordamida zararli dasturlarni tekshirishi kerak.

Axborot tashuvchi va saqlovchi qurilmalarini olib chiqish uchun ruxsatnomada quyidagilar ko'rsatilishi kerak:

- to'liq F.I.Sh va qurilmadan foydalanadigan xodimning lavozimi;
- qurilmaning modeli va qayd raqami;
- olib chiqish sababi (xizmat safarlar, uchrashuvlar, muzokaralar va boshqalar);
- ruxsatnomaning amal qilish muddati.

Konfidensial ma'lumotlarni saqlash uchun ishlatiladigan ma'lumotlarni saqlovchi va tashuvchi qurilmalarni boshqariladigan zonadan tashqariga olib chiqishga yo'l qo'yilmaydi.

12. Konfidensial ma'lumotlarni saqlash uchun ishlatiladigan ma'lumotlarni saqlovchi va tashuvchi tashqi qurilmalar lokal tarmoq administratori tomonidan ushbu Yo'riqnoma ilovasida keltirilgan jadvalga muvofiq ro'yxatga olinadi.

13. Konfidensial ma'lumotlarni saqlash uchun ishlatiladigan ma'lumotlarni saqlovchi va tashuvchi tashqi qurilmalar so'zlari bilan yoki boshqa turli taniqli belgi bilan belgilangan bo'lishi kerak.

14. Konfidensial ma'lumotlarni saqlash uchun ishlatiladigan ma'lumotlarni saqlovchi va tashuvchi tashqi qurilmalar lokal tarmoq administratori tomonidan inventarizatsiya qilinishi kerak.

Axborot tashuvchisi va ularda markirovkaning mavjudligini tekshirish lokal tarmoq administratori tomonidan yiliga kamida bir marta amalga oshiriladi.

15. Jamiyat xodimlari axborot tashuvchi va saqlovchi vositalardan foydalanishda quyidagi talablarga rioya qilishlari shart:

- vositalardan faqat o'zlarining ish faoliyatiga oid vazifalarini bajarish uchun foydalanishi;
- lokal tarmoq administratoriga ushbu yo'riqnoma talablarining buzilishining har qanday faktlari to'g'risida xabar berish;
- ma'lumotlarni saqlash qurilmalari va axborot tashuvchi va saqlovchi vositalarni yo'qotish (o'g'irlash) yoki ishlamay qolish faktlari to'g'risida lokal tarmoq administratoriga xabar berish;
- axborot tashuvchi va saqlovchi vositalarining jismoniy xavfsizligini barcha oqilona usullar bilan ta'minlash;
- axborot tashuvchilarni boshqa shaxslarga bermaslik.

16. Axborot tashuvchi va saqlovchi vositalardan foydalanishda Jamiyat xodimlariga ularni xavfsizligini ta'minlash choralari ko'rilmagan bo'lsa, ularni qarovsiz qoldirish taqiqlanadi.

17. Agar ishchi stansiyani yoki serverni uchinchi shaxslar ta'mirlashni talab qilsa, ta'mirlashni boshlashdan oldin ma'lumotlarni saqlash qurilmasi (HDD) ma'lumotlardan tozalanishi kerak. Ushbu ta'mirlash ishlari lokal tarmoq administratori tomonidan nazorat qilinishi kerak.

18. Jamiyatning xodimlari telefon so'zlashuvlari davomida konfidensial ma'lumotlar haqida so'zlashishlari ta'qiqlanadi.

Vositalarni hisobdan chiqarish va yo'q qilish tartibi

19. Agar xodim ishdan bo'shatilgan yoki boshqa ish joyiga o'tkazilgan bo'lsa, unga berilgan Jamiyatga tegishli bo'lgan tashuvchi, saqlovchi va mobil qurilmalar Bo'limga topshirilishi shart.

20. Ishlamay qolgan yoki yo'q qilishga mo'ljallangan tashuvchi, saqlovchi va mobil qurilmalar qulflanadigan metall shkaflarda (seyflarda) saqlanishi kerak.

21. Axborot tashuvchi, saqlovchi va mobil qurilmalardan foydalanishni bekor qilish to'g'risida qaror qabul qilingandan so'ng, ularni yo'q qilish (utilizatsiya) to'g'risida bayonnoma tuzish orqali amalga oshirilishi kerak.

22. Foydalanish uchun yaroqsiz bo'lgan tashuvchi, saqlovchi va mobil qurilmalarni formatlash va ularni jismoniy yo'q qilish orqali tozalanishi kerak.

23. Konfidensial ma'lumotga ega bo'lmagan tashuvchi, saqlovchi va mobil qurilmalarni boshqa xodimga berishda ushbu qurilmalarda saqlanadigan barcha ma'lumotlarni uni formatlash orqali o'chirib yo'q qilinishi kerak.

24. Agar ma'lumotlarni tashuvchi, saqlovchi va mobil qurilmalardan konfidensial ma'lumotlardan tozalash zarur bo'lsa, axborotni kafolatlangan yo'q qilish vositalaridan foydalanish va ushbu vositalarga ega bo'lgan ixtisoslashtirilgan tashkilotlarning xizmatlariga murojat qilish kerak.

Mobil qurilmalar, ma'lumot saqlovchi va tashuvchi qurilmalar bilan ishlashda axborot xavfsizligini ta'minlash bo'yicha yo'riqnomaga 1–ilova

_____

_____ rahbari/o'rinbosari

_____

(lavozimi, unvoni, F.I.Sh.)

20___ yil "____" _____

"O'zbekiston milliy elektr tarmoqlari" AJ hududiga mobil qurilmalar, ma'lumot saqlovchi va tashuvchi qurilmalarni (ma'lumot to'plagichlar, noutbuk va h.k.) olib kirish yoki hududdan olib chiqish uchun ruxsat berishga BILDIRGI

Xizmat zarurati tufayli, Sizdan ko'rsatib o'tilgan xodimga Mobil qurilmalar, ma'lumot saqlovchi va tashuvchi qurilmalarni _____ binosi hududiga olib kirish / hududdan olib chiqish uchun ruxsat berishingizni so'rayman.

_____,

F.I.Sh.

_____ _____

(lavozimi,) (bo'lim nomi)

Tel:_____, _____

(olinadigan axborot tashuvchisi)

_____

_____ boshlig'i:

_____

(lavozimi, o'nvoni)

20__ y. . _____ _____

F.I.Sh

Kelishildi:

Raqamlashtirish boshqarmasi boshlig'i: _____

Ishlar yuritish boshqarmasi: _____

Mobil qurilmalar, ma'lumot saqlovchi va tashuvchi qurilmalar bilan ishlashda axborot xavfsizligini ta'minlash bo'yicha yo'riqnomaga 2–ilova

Yo'q qilishga ruxsat beraman

_____ rahbari

_____

(lavozimi, unvoni, F.I.Sh.)

_____

20____ yil "___" _____

_____-sonli

Mobil qurilmalar, ma'lumot saqlovchi va tashuvchi qurilmalarni yo'q qilinganligi to'g'risidagi

DALOLATNOMA

_____

(lavozimi, unvoni, F.I.Sh.)

_____

_____ tarkibidagi komissiya

_____ ga asos, yo'q qilish uchun quyidagi axborot tashuvchi vositasini tanlab oldi:

T/R	Ro' yxatga olish raqami	Maxfiylik belgisi	Echib olinadigan tashuvchilarni (ma' lumot to' plagichlar)	Tashuvchi turi	Tashuvchini yo' q qilish bo' yicha amalga oshirilgan harakat	Izoh

Jami bo'lib _____ axborot tashuvchi vositalari

(soni, yozuv bilan)

yo'q qilindi.

Komissiya a'zolari:

_____ _____

(imzo) (F.I.Sh.)

_____ _____

(imzo) (F.I.Sh.)

1.7 Tashqi foydalanuvchilar bilan munosabatlarda xavfsizlik choralari

1. Tashqi foydalanuvchilar bilan munosabatlarda xavfsizlik choralari quyidagilarga qaratilgan:

- Jamiyat va uning vositalarini himoya qilish obyektlariga tashqi foydalanuvchilarning ruxsatsiz jismoniy kirishini istisno qilish;
- Jamiyat axborot resurslariga kirishda tashqi tashkilotlarning foydalanuvchilari tomonidan ruxsatsiz tarmoqqa kirishni istisno qilish.

2. Tashqi foydalanuvchilar bilan ishlashda xavfsizlik choralariga quyidagilar kiradi:

- Jamiyatga tashrif buyuruvchilarning kelishi va ketishi jurnalini yuritish;
- Jamiyat xodimlari tomonidan bino ichida mehmonlarni kuzatib borish;
- tashrif buyuruvchilarni va uchinchi tomon tashkilotlarini alohida qabul xonalarida qabul qilish;

3. Jamiyat uchun dasturiy ta'minot va uskunalarni ishlab chiqish, texnik xizmat ko'rsatish yoki yetkazib berish bilan shug'ullanuvchi uchinchi tomon tashkilotlari bilan tuzilgan shartnomalarda konfidensial ma'lumotlarni uchinchi shaxslarga tarqatmaslik talablarini belgilash.

4. Ishlab chiquvchilar, uskunalarni yetkazib beruvchilar va shu kabi uchinchi tomon tashkilotlari xodimlari Jamiyatning himoya qilinadigan obyektlariga kirishni ta'minlashda ular bilan tuzilgan shartnomalarda "konfidensial ma'lumotlarni oshkor etmaslik" shartlari va talablari qat'iy belgilash. Shuningdek, uchinchi tomon tashkiloti tomonidan himoya obyektlariga kirish huquqini beradigan aniq shaxslar ro'yxati aniqlanishi lozim va bunday ruxsat faqat shu shaxslarga berilishi shart.

5. Jamiyat muhofaza qilish obyektlariga qabul qilingan uchinchi tomon tashkilotlari vakillari Jamiyat xodimi huzurida bo'lishi va o'ziga tegishli vazifani bajarishi shart.

6. Uchinchi tomon tashkilotlari bilan o'zaro aloqalarda xavfsizlikni ta'minlash choralarini ko'rish. (1C: Buxgalteriya tizimlarini Xizmat ko'rsatuvchi bank serveriga ulaganda) ushbu Siyosatning 1-ilovasida keltirilgan Lokal tarmoq va xavfsiz tarmoq ulanishlarini tashkil etish to'g'risidagi Nizom talablariga muvofiq xavfsiz ulanishlarni tashkil qilishni o'z ichiga oladi.

7. Jamiyatning resurslariga kirishda tashqi foydalanuvchilarning tarmoqdan ruxsatsiz kirishini istisno qilish maqsadida, ushbu siyosatning 2-ilovasida keltirilgan "Tarmoq infratuzilmasi va tarmoqlararo ekran darajasida axborot xavfsizligini ta'minlash to'g'risida nizom"ga muvofiq, shuningdek, Jamiyatning axborot resurslariga kirishda foydalanuvchining autentifikatsiyasi, siyosatning 7-ilovasida keltirilgan "Parol bilan himoya qilish bo'yicha yo'riqnoma"ga muvofiq amalga oshiriladi.

1.8 Axborot xavfsizligi insidentlariga munosabat

1. Axborot xavfsizligining quyidagi insidentlari qayd etilishi va hisobga olinishi kerak:

- ma'lumotlarning konfidensialligi, yaxlitligi va mavjudligini buzilishi;
- texnologik jarayonning buzilishi;

- favqulodda vaziyatlar (yong‘inlar, toshqinlar va boshqa tabiiy ofatlar yoki ishlab chiqarishdagi baxtsiz hodisalar);

- Jamiyatda tashqi tarmoqlar bilan aloqaning yo‘qolishi;

- har qanday sababga ko‘ra asosiy tarmoq, server uskunalari, axborotni himoya qilish vositalari, ham texnik, ham dasturiy ta’minotning ishlamay qolishi;

- axborot resurslari dasturiy ta’minotining noto‘g‘ri ishlashi;

- uchinchi shaxslarning axborot manbalariga ruxsatsiz kirishi;

- ma’lumotlarni qayta ishlash, saqlash, uzatish bo‘yicha har qanday qoidalarning buzilishi;

- DoS (Denial of Servise) va DDoS (Distributed Denial of Servise) hujumlar;

- himoya vositalari yordamida aniqlangan tarmoq hujumlari;

- lokal tarmoqda, serverlarda va ularga o‘rnatilgan dasturiy ta’minotda axborot xavfsizligi vositalaridagi nosozliklar;

- g‘ayritabiiy tarmoq faoliyati va g‘ayritabiiy dastur harakati;

- yangi tarmoq tugunlarini ulash va yangi xizmatlarning paydo bo‘lishi;

- ma’lumot tashuvchilar va ma’lumotlarning yo‘qolishi va o‘g‘irlanishi;

- zaifliklarning paydo bo‘lishi;

- apparat konfiguratsiyasini, sozlamalari va axborot xavfsizligi parametrlarini o‘zgartirish;

- ma’lumot to‘plash bo‘yicha noqonuniy harakatlar aniqlanishi;

- aniqlangan xavfli viruslar va zararli dasturlar;

- muhofaza qilinadigan ma’lumotlarning tarqalishi, o‘chirilishi, noqonuniy kirishi;

- ushbu axborot xavfsizligi siyosatida belgilangan qoidalarning buzilishi.

Jamiyatning boshqa xodimlari, axborot xavfsizligi bilan bog‘liq hodisa yuz bergan taqdirda, Raqamlashtirish boshqarmasi yoki Axborot va kiberxavfsizlik bo‘limi ma’sul xodimlariga xabar berishlari shart.

2. Axborot xavfsizligining muhim nomaqbul va salbiy oqibatlariga olib keladigan axborot xavfsizligi hodisalari yuz berganda, ular haqida Jamiyat rahbariyatiga xabar berish shart.

1.9 Aloqa kanallarining xavfsizligini ta’minlash

Jamiyat binosida axborotlashtirish obyektlari sirasiga kiruvchi hududlar mavjud bo‘lganligi tufayli, jamiyat axborotlashtirish obyektlarida axborot xavfsizligi qoidalari va talablariga muvofiq Wi-Fi tarmog‘idan foydalanish mumkin emas.

1. Jamiyatning Wi-Fi tarmog‘i alohida VLAN orqali tashkil etilgan bo‘lib, Jamiyat rahbariyati, xodimlari (ro‘yhat bilan) va Jamiyatga tashrif buyuruvchi mehmonlarning shaxsiy qurilmalarini internet tarmog‘iga ulanish maqsadida joriy etilgan.

2. Jamiyat joylashgan binoda ichki foydalanish uchun simsiz Wi-Fi tarmog‘i quyidagi talablarga javob berish kerak:

- Wi-Fi tarmog‘i ko‘rinmas (скрытый) qilinishi;

- Wi-Fi tarmog‘iga ulanish uchun barcha qurilmalar MAC – manzili ro‘yxatga kiritilishi kerak;

- xodimlarning shaxsiy qurilmalarini Wi-Fi tarmog'i orqali (ish stansiyalari, noutbuklar, planshetlar va uyali telefonlar va boshqalar) ichki tarmoq resurslariga, xususan Korporativ tarmoq va axborot tizimlariga ulashni ta'qiqlash;

- xavfsizlikni ta'minlash maqsadida Korporativ tarmoqqa oldin ulangan terminallarni (ish stansiyalari va noutbuklarni) ichki Wi-Fi tarmog'iga ikkinchi kirish huquqi bilan ta'minlash taqiqlanadi (qat'iy belgilangan individual terminal qurilmalari Wi-Fi tarmoqlariga ulanishi kerak).

1.10 Axborotni kriptografik himoya qilishni tashkil etish bo'yicha yo'riqnoma

Ushbu Yo'riqnoma axborotni kriptografik muhofaza qilishning asosiy chora-tadbirlarini, usullarini va vositalarini belgilaydi, shuningdek, Jamiyatda axborotlarni kriptografik himoya vositalari va elektron raqamli imzo kalitlari (ERI) bilan ishlashga vakolatli xodimlarining harakatlarini tartibga soladi.

Raqamlashtirish boshqarmasi boshlig'i axborot xavfsizligi administratori bilan birgalikda Jamiyatda E-xat tizimidan foydalangan holda axborotning kriptografik himoyasini tashkil etish shuningdek himoyalangan ulanishlarni tashkil etish va boshqarish bo'yicha belgilangan talablarning bajarilishini nazorat qiladi.

Jamiyatda ma'lumotlarning tizim orqali himoyalangan uzatilishini ta'minlash maqsadida AKHVdan himoyalangan elektron pochta E-xat va edo.ijro ijro tizimida foydalaniladi.

E-xat himoyalangan elektron pochtasi foydalanuvchilari faqat Jamiyatning devonxona bo'limi xodimlari, edo.ijro intizomi tizimidan foydalanuvchilar esa faqat Jamiyatning tarkibiy bo'linmalari boshliqlari va Jamiyat rahbariyati rahbarlari hisoblanadi.

Raqamlashtirish boshqamasi va Ishlarni yuritish boshqarmasi E-xat tizimida ishlash uchun "UNICON.UZ" MChJ shaxsiy ERI kalitlari va ochiq ERI kalitlari sertifikatlarini olish uchun javobgardir.

E-xat tizimida kriptografik kalitlar bilan ishlaydigan foydalanuvchilar quyidagilarga majbur:

- shaxsiy ERI kalitlarining USB tashuvchisi bilan birga xavfsizligini ta'minlash va foydalanilmagan taqdirda ularni faqat foydalanuvchining o'zi kirishi mumkin bo'lgan himoyalangan joylarda (seyflarda) saqlash;

- foydalanuvchi yo'qligida yoki E-xat tizimida ishlamayotganda kriptografik kalitlarni ish joyida qarovsiz qoldirmaslik;

- Markaziy apparat lokal tarmog'i administratori yoki Raqamlashtirish boshqarmasini kriptografik kalit yo'qolishi yoki o'g'irlanishi, kriptografik kalitning buzilishi, kriptografik kalit tashuvchisining shikastlanishi, tizimlarga kirishdagi muammolarda xabardor qilish;

- ishdan bo'shash yoki AKHV va ERI bilan bog'liq vazifalarni bajarishdan ozod qilish paytida kriptografik kalit saqlash USB - vositasini topshirish;

- berilgan kriptografik kalitlarni saqlash USB - vositasidan boshqa maqsadlarda ishlatmaslik.

Ishdan chiqqan kriptografik kalitlar yoki ularning saqlash USB - vositalari Ishlarni yuritish boshqarmasiga belgilangan tartibda almashtirish uchun qaytariladi.

Javobgarlik taqsimoti

Ushbu Siyosat Jamiyatda axborot xavfsizligini ta'minlash uchun quyidagi javobgarlikni taqsimlaydi:

- Axborot va kiberxavfsizlik bo'limi boshlig'i Jamiyatda axborot xavfsizligini ta'minlash bo'yicha barcha tadbirlar uchun javobgardir;
- xodimga ishonib topshirilgan har qanday shakldagi ma'lumotni saqlash va uni himoya qilishning tegishli darajasini ta'minlash uchun ushbu xodim shaxsiy javobgarlikni o'z zimmasiga oladi;
- Jamiyat axborot resurslarida amalga oshirilgan harakatlar uchun Jamiyat xodimlari o'zlariga yuklatilgan vazifalar doirasida javobgardirlar;

Jamiyatning ishchi stansiyasi xizmat vazifalarini bajarish uchun taqdim etilgan xodimi ishchi stansiyaning axborot xavfsizligi (shu jumladan jismoniy) uchun javobgardir;

- Jamiyat binosida jismoniy joylashtirilgan lokal tarmoqning axborot xavfsizligi uchun lokal tarmoq administratori, Jamiyatning tizim tashkilotlarida esa har bir korxonada tayinlangan (tarmoqlar, korxonalardagi serverlar va ish stansiyalariga xizmat ko'rsatuvchi) axborot xavfsizligi administratorlari javobgar.

Ma'sul shaxs ishda bo'lmaganida (ta'til, kasallik, mehnat safari va boshqalar) uning vazifalarini belgilangan tartibda tayinlangan shaxs bajaradi. Ushbu shaxs tegishli huquqlarga ega bo'ladi va o'ziga yuklatilgan vazifalarning to'g'ri bajarilishi uchun javobgardir.

Jamiyat xodimlarining axborot xavfsizilgi siyosatida belgilangan talablarni buzish va bajarmaslik holatlarda, aybdor xodimlarga nisbatan jazo choralarini qo'llashga (mukofat puli, ustama pulidan maxrum qilish, jarima solish va b.sh) sabab bo'ladi. O'zbekiston Respublikasining mehnat qonunchiligiga va ichki mehnat tartib qoidalariga muvofiq ta'sir choralarini ko'rishga va intizomiy javobgarlikka tortishga sabab bo'ladi.