Ilmiy rahbar: Yunusov Azizbek Fazilovich
Andijon davlat pedagogika instituti "Aniq fanlar" fakulteti, Matematika va informatika kafedrasi o'qituvchisi
Abdumannobov Diyorbek Abdullajon o'g'li
Abdullajonov Mo'minjon Xayrullo o'g'li
Andijon davlat pedagogika instituti "Aniq fanlar" fakulteti,
Matematika va informatika 3-bosqich talabasi
Olimovolim616@gmail.com
+998996372865
Mominjonabdullajonov38@gmail.com
+998334049125

AXBOROT XAVFSIZLIGINI TA'MINLASH VA AXBOROT XAVFSIZLIGI SIYOSATI

Annotatsiya: Axborot xavfsizligini ta`minlash orqali,butun insoniyatga xavf solayotgan axborot xatarining oldini olish,uning sabablarini o'rganib chiqish va uni tushuntirshdan iborat.Axborot xavfsizligi ta`minlansa nafaqat shaxsiy,balki butun jamiyatning axborot sohasidagi xavfsizligini himoyalash mukin. Hozirgi kunda mamlakatimizda axborot bormoqda,shuningdek,taxdidlar ham talaygina.Ularning insoniyatga ziyoni oshib bormoqda. Axboroti himoyalash obyektlarda axborot xavfsizligini ko'p sonli mumkin bo'lgan xavflardan himoya qilish uchun yaratiladi. Ularning ba'zi birlari axborotni bir vaqtning o'zida bir nechta xavflardan himoya qiladi. Axborotni himoya qilishning huquqiy usullaridir, bu ixtiyoriy vazifali himoya qilish tizimini rasmiy ravishda kurishni va ishlatishni asosi bo'lib xizmat qiladi; bu tashkiliy usullardir, ular odatda bir nechta xavflarni bartaraf (qaytarish) etish uchun ishlatiladi;bu texnik , ular tashkiliy va texnik tadbirlarga asoslangan holda ko'pchilik xavflardan axborotlarni himoya qilish tushuniladi.

Kalit so`zlar: Axborot, organizational security policy, AT kontseptsiyasi, GOST R ISO/IEC, axborot siyosati, xavfsizlik siyosati, foydalanish siyosati, zaxira siyosati, audit.

Kirish: Axborotning muhimlik darajasi qadim zamonlardan ma'lum. Shuning uchun ham qadimda axborotni himoyalash uchun turli xil usullar qo'llanilgan. Ulardan biri– sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o'qiy olmagan. Asrlar davomida bu san'at – sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixona rezidentsiyalari va razvedka missiyalaridan tashqariga chiqmagan. Faqat bir necha o'n yil oldin hamma narsa tubdan o'zgardi, ya'ni axborot o'z qiymatiga ega bo'ldi va keng tarqaladigan mahsulotga aylandi. Uni endilikda ishlab chiqaradilar, saqlaydilar, uzatishadi, sotadilar va sotib oladilar. Bulardan tashqari uni o'g'irlaydilar, buzib talqin etadilar va soxtalashtiradilar. Shunday qilib, axborotni himoyalash zaruriyati tug'iladi. Axborotni qayta ishlash sanoatining paydo bo'lishi axborotni himoyalash sanoatining paydo bo'lishiga olib keladi. Muayyan axborot tizimining axborotni himoya qilish texnologiyasini tavsiflash uchun odatda axborot xavfsizligi siyosati yoki ko'rib chiqilayotgan axborot tizimining xavfsizlik siyosati yaratiladi. Tashkiliy xavfsizlik siyosati (inglizcha: *Organizational security policy*) – tashkilot faoliyatida axborot xavfsizligi sohasidagi hujjatlashtirilgan qoidalar, tartiblar, amaliyotlar yoki ko'rsatmalar to'plami.

Axborot va telekommunikatsiya texnologiyalari xavfsizligi siyosati (inglizcha: *ICT security policy*) – tashkilot va uning axborot va telekommunikatsiya texnologiyalari ichida aktivlarni, shu jumladan muhim ma'lumotlarni boshqarish, himoya qilish va tarqatish usullarini belgilaydigan qoidalar, ko'rsatmalar, o'rnatilgan amaliyotlar.

Axborot xavfsizligi siyosatini shakllantirishda axborot tizimini himoya qilishning quyidagi yo‘nalishlarini alohida ko‘rib chiqish tavsiya etiladi.

- Axborot tizimi ob’ektlarini himoya qilish;
- Jarayonlar, protseduralar va axborotni qayta ishlash dasturlarini himoya qilish;
- Aloqa kanallari (akustik, infraqizil, simli, radiokanallar va boshqalar)ni himoya qilish, shu jumladan mahalliy tarmoqlarda axborotni himoya qilish;
- Yon elektromagnit nurlanishni bostirish;
- Himoya tizimini boshqarish.

Shu bilan birga, yuqoridagi sohalarning har biri uchun axborotni himoya qilish vositalarini yaratishda axborot xavfsizligi siyosati quyidagi bosqichlarni tavsiflashi talab etiladi:

- Himoya qilinadigan axborot va texnik resurslarni belgilash;
- Potensial tahdidlarning to‘liq to‘plami va ma’lumotlarning sizib chiqish kanallarini aniqlash;
- Turli xil tahdidlar va sizib chiqish kanallari mavjud bo‘lganda ma’lumotlarning zaiflik darajasi va xavflarini baholashni o‘tkazish;
- Himoya tizimiga qo‘yiladigan talablarni aniqlash;
- Axborot xavfsizligi vositalari va ularning xususiyatlarini tanlashni amalga oshirish;
- Tanlangan himoya choralari, usullari va vositalarini amalga oshirish va ulardan foydalanishni tashkil etish;
- Butunlikni nazorat qilish va himoya qilish tizimini boshqarishni amalga oshirish.

Axborot xavfsizligi siyosati axborot tizimiga qo‘yiladigan hujjatlashtirilgan talablar shaklida tuziladi. Hujjatlar, odatda, himoya jarayonining tavsifi (tafsiloti) darajalariga ko‘ra darajalarga bo‘linadi. Axborot xavfsizligi siyosatining yuqori darajadagi hujjatlari tashkilotning axborot xavfsizligi sohasidagi faoliyatiga nisbatan pozitsiyasini, ushbu sohadagi davlat, xalqaro talablar va standartlarga rioya qilish istagini aks ettiradi. Bunday hujjatlar „AT kontseptsiyasi“, „AT boshqaruvi reglamenti“, „AT siyosati“, „AT texnik standarti“ va boshqa tashqi va ichki foydalanish deb nomlanishi mumkin. GOST R ISO/IEC 17799-2005ga muvofiq, axborot xavfsizligi siyosatining yuqori darajasida quyidagi hujjatlar tuzilishi kerak: „AT xavfsizligi kontseptsiyasi“, „Axborot tizimi resurslaridan maqbul foydalanish qoidalari“, „Biznesning uzluksizlik rejasi“.

O‘rta darajaga axborot xavfsizligining ayrim jihatlari bilan bog‘liq hujjatlar kiradi. Bu axborot xavfsizligi vositalarini yaratish va ulardan foydalanish, shuningdek, axborot xavfsizligining ma’lum bir sohasida tashkilotning axborot va biznes jarayonlarini tashkil etish talablaridir. Bunga misol qilib ma’lumotlar xavfsizligi, aloqa xavfsizligi, kriptografik himoya vositalaridan foydalanish, kontentni filtrlash va boshqalarni keltirish mumkin. Bunday hujjatlar odatda tashkilotning ichki texnik va tashkiliy siyosati (standartlari) shaklida nashr etiladi. O‘rta darajadagi axborot xavfsizligi siyosatining barcha hujjatlari maxfiy hisoblanadi.

Axborot xafsizligini ta’minlashda quyidagi siyosat va tartiblarni ishlab chiqish lozim:

Axborot siyosati. Maxfiy ma’lumotlarni va ularni qayta ishlash, saqlash, uzatish va yo‘q qilish usullarini oshkor qiladi.

Xavfsizlik siyosati. Turli xil kompyuter tizimlari uchun texnik boshqaruvni belgilaydi.

Foydalanish siyosati. Kompyuter tizimlaridan foydalanish bo‘yicha kompaniya siyosatini ta’minlaydi.

Zaxira siyosati. Kompyuter tizimlarining zaxira nusxasini yaratish uchun talablarni belgilaydi.

Hisobni boshqarish tartib-qoidalari. Foydalanuvchilar qo‘shilgan yoki o‘chirilganda bajarilishi kerak bo‘lgan amallarni belgilaydi.

Favqulodda vaziyatlar rejasi. Tabiiy ofatlar yoki inson tomonidan sodir etilgan hodisalardan keyin kompaniya jihozlarini tiklash bo‘yicha harakatlarni ta’minlaydi.

Xavfsizlik siyosatini amalga oshirish texnik vositalar va to‘g‘ridan-to‘g‘ri nazorat qilish vositalarini amalga oshirishdan, shuningdek, xavfsizlik xodimlarini tanlashdan iborat. Xavfsizlik bo‘limi doirasidan tashqarida tizimlar konfiguratsiyasiga o‘zgartirishlar kiritish talab qilinishi mumkin, shuning uchun tizim va tarmoq ma’murlari xavfsizlik dasturini amalga oshirish ishlarida ishtirok etishlari kerak.Har qanday yangi xavfsizlik tizimlaridan foydalanganda malakali xodimlar mavjud bo‘lishi kerak. Tashkilot o‘z xodimlarining ishtirokisiz maxfiy

ma’lumotlarning himoyasini ta’minlay olmaydi. Vakolatli kasbiy qayta tayyorlash bu xodimlarni zarur ma’lumotlar bilan ta’minlash mexanizmi hisoblanadi.

Xodimlar xavfsizlik masalalari nima uchun juda muhim ekanligini bilishlari va maxfiy ma’lumotlarni aniqlash va himoya qilish uchun o‘qitilishi kerak.

Audit axborot xavfsizligini joriy etish jarayonining oxirgi bosqichidir. U tashkilot ichidagi axborot xavfsizligi holatini, tegishli siyosat va tartiblarni yaratishni, texnik nazoratni faollashtirishni va xodimlarni tayyorlashni belgilaydi.

Axborotni himoyalash bugungi kunda har bir korxonaning dolzarb masalasi hisoblanadi. Axborot xavfsizligi hodisalari tufayli keladigan zarar tashkilot taqdiriga sezilarli ta’sir ko‘rsatishi mumkin. Axborot xavfsizligini ta’minlashning ko‘plab usullari va sohalari mavjud. Bugungi maqolamizda tashkilotlarda axborot xavfsizligini ta’minlashning asosiy hujjati sanalmish axborot xavfsizligi hujjati to‘g‘risida so‘z yuritiladi.

Ta’kidlaganimizdek, tashkilotda axborot xavfsizligini ta’minlashni samarali tashkil etish vositalaridan biri bu axborot xavfsizligi siyosatini joriy etishdir. Xo‘sh, axborot xavfsizligi siyosati nima, u qanday joriy etiladi va joriy qilishdan maqsad nimalardan iborat?

Axborot xavfsizligi siyosatining ko‘plab ta’riflari turli hujjatlarda keltirilgan, shulardan davlat organlari uchun mos keluvchi ta’rif shunday: axborot xavfsizligi siyosati – bu korxona yoki tashkilot xodimlari axborot resurslarini himoya qilish uchun kundalik amaliyotida amal qiladigan chora-tadbirlar, qoidalar va tamoyillar to‘plami.

Axborot xavfsizligi ishlab chiqish asoslari:

Axborot xavfsizligi siyosati, birinchi navbatda, korxonada axborot xavfsizligini ta’minlashning maqsad va vazifalarini faoliyatga singdirish uchun zarurdir. Faoliyat yuritayotgan har bir xodim shuni tushunishi kerakki, xavfsizlik xodimi nafaqat ma’lumotlar chiqib ketishini tekshiruvchi, balki kompaniya xatarlarini minimallashtirish va shu sababli kompaniya rentabelligini oshirishda yordamlashuvchidir.

Yurtimizda elektron hukumatni qurish, davlat organlari faoliyatini raqamlashtirish bilan bog‘liq harakatlar jadal sur’atlarda amalga oshirilmoqda. Hukumatning tegishli qarorlari va axborot xavfsizligi sohasidagi standartlarga (O‘z DSt ISO/IEC 270XX) muvofiq har bir tashkilotda

axborot xavfsizligi siyosatini ishlab chiqish va joriy qilinishi lozimligi yuzasidan talablar keltirilgan. Xususan, O‘z DSt ISO/IEC 27002 standartining 5-bobida Axborot xavfsizligi siyosatini ishlab chiqish bo‘yicha talablar belgilab qo‘yilgan.

O‘zbekiston Respublikasi hududida davlat va xo‘jalik boshqaruvi organlarida, shuningdek, mahalliy davlat hokimiyati organlarida (bundan buyon matnda tashkilotlar deb yuritiladi) axborot xavfsizligi siyosatini ishlab chiqish va amalga oshirishning asosiy tamoyillari va tartibini belgilovchi «O‘zbekiston Respublikasi hududida axborot xavfsizligi siyosatini ishlab chiqish bo‘yicha uslubiy qo‘llanmalar» ham 2013–2020 yilllarda O‘zbekiston Respublikasi Milliy axborot-kommunikatsiya tizimini rivojlantirishni muvofiqlashtirish bo‘yicha Respublika komissiyasining 2016-yil 23-fevraldagi 7-bayoni bilan tasdiqlangan. Uslubiy qo‘llanma tashkilotda xavfsizlikni boshqarish bo‘yicha amaliy choralarni tanlash, shuningdek, tashkilotlar o‘rtasida ma’lumotlar almashishda ularning yaxlitligi, qulayligi va maxfiyligini ta’minlash uchun asosdir.

Axborot xavfsizligi siyosatini ishlab chiqish bosqichlari:

Mavjud uslubiy qo‘llanmaga muvofiq axborot xavfsizligi siyosatini (keyinchalik matnda – Siyosat) ishlab chiqish uch bosqichda amalga oshiriladi.

Siyosatni ishlab chiqish uchun ishchi guruh tashkilot rahbarining buyrug‘i bilan tasdiqlanadi, unda quyidagi shaxslar bo‘lishi kerak:

- tashkilot rahbariyati vakili;

- axborot xavfsizligi masalalari bo‘yicha mas’ul,

- kadrlar bo‘limi boshlig‘i (HR xizmati);

- texnik bo‘linmalar vakillari (axborot xavfsizligi ma’muri, tarmoq ma’muri, ma’lumotlar bazasi ma’muri yoki boshqa vakolatli xodimlar). Zaruriyatga qarab, tashkilotning boshqa xodimlarini, uchinchi tomon ixtisoslashtirilgan tashkilotlarini yoki mutaxassislarni jalb qilish mumkin.

Siyosatni ishlab chiqish tartibi quyidagi bosqichlarga bo‘linadi:

Birinchi bosqich. Dastlabki xavfsizlik auditi, shu jumladan, axborot xavfsizligi holatini dastlabki o‘rganish va inventarizatsiya qilish, tashkilot xavfsizligiga tahdidlarni aniqlash, himoya qilinishi lozim resurslarni aniqlash, risklarni aniqlash.

Audit jarayonida axborot xavfsizligining hozirgi holatini tahlil qiladi, mavjud zaifliklarni, faoliyatning eng muhim sohalari va tashkilotning xavfsizlikka tahdid jarayonlariga eng sezgir yo‘nalishlari aniqlanadi.[1]

Audit tashkilotning axborot xavfsizligining tahdidlari va zaifliklarini aniqlashga, siyosatni ishlab chiqish uchun dastlabki ma’lumotlarni olishga, shuningdek, tashkilotni axborotlashtirish ob’yektlarini keyingi sertifikatlashga tayyorlashga imkon beradi.

Tashkilot auditi davomida quyidagilar amalga oshiriladi:

- tashkilotning O‘zbekiston Respublikasi qonunchiligi, O‘zbekiston Respublikasi Prezidenti va O‘zbekiston Respublikasi Vazirlar Mahkamasining farmon va qarorlari talablariga muvofiqligi o‘rganiladi va tahlil qilinadi, O‘zbekiston Respublikasining normativ-huquqiy hujjatlari toifalarga taqsimlanishi, shuningdek, tashkilotda axborot xavfsizligi masalalarini tartibga soluvchi normativ hujjatlarning ijrosi o‘rganiladi;

- tashkilotning kompyuterlari va serverlarini dastlabki tekshirish, ya’ni ishlatilgan operatsion tizimlarning sozlamalari, dastur va tizim dasturlari (dasturiy ta’minot), axborot xavfsizligi vositalari, shuningdek, axborot-kommunikatsiya

texnologiyalariga kiritilgan boshqa qo‘shimcha qurilmalar va boshqalar tahlil qilinadi;

- axborot xavfsizligining tahdidlari va zaifliklari uchun tashkilot veb-sayti tahlil qilinadi;

- tashkilot hududi, perimetri va binolarining jismoniy himoya qilishni ta’minlash bo‘yicha amalga oshirilgan chora-tadbirlar tahlil qilinadi, ya’ni xavfsizlik tizimi, kirishni boshqarish vositalari, yong‘in xavfsizligi tizimlari va boshqalar;

- suhbat orqali tashkilot xodimlarining tashkilotda o‘rnatilgan axborot xavfsizligi qoidalari to‘g‘risida xabardorligi baholanadi;

- tashkilotning axborot va moddiy resurslarini turkumlash va inventarizatsiya qilish tahlili amalga oshiriladi.

Ikkinchi bosqich. Tashkilotning axborot xavfsizligi siyosati loyihasini ishlab chiqish. Siyosatni ishlab chiqishda quyidagi asosiy qoidalarga rioya qilish talab etiladi:

- siyosat amaldagi qonunchilikka va davlat standartlari talablariga to‘liq mos bo‘lishi lozim;

- siyosat matnida ikki tomonlama talqin qilishga imkon bermaydigan aniq va bir ma’noli jumlalar bo‘lishi lozim.

Umuman olganda, siyosat axborot tizimlari va axborot xavfsizligi vositalarini amalga oshirishda va ulardan foydalanishda, shuningdek, ma’lumot almashish va axborotni qayta ishlash operatsiyalarini bajarishda foydalanuvchilar, ma’murlar va boshqa mutaxassislarning talab qilinadigan xatti-harakatlari to‘g‘risida aniq tasavvur berishi kerak.

Siyosat – bu tashkilotning barcha manfaatdor tomonlariga cheklovlarsiz taqdim etilishi mumkin bo‘lgan ommaviy hujjat.

Uchinchi bosqich. Tashkilotning axborot xavfsizligi siyosatini muvofiqlashtirish va amalga oshirish.

Ishlab chiqilgan siyosat loyihasi tegishlicha O‘zbekiston Respublikasi axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligiga va vakolatli organlarga tasdiqlash uchun yuboriladi hamda tasdiqlangandan so‘ng tashkilot rahbarining buyrug‘i bilan kuchga kiradi. Shu bilan birga, tasdiqlangan siyosatni to‘liq amalga oshirish uchun aniq sanalar va ijrochilar bilan siyosatni amalga oshirish bo‘yicha tarmoq harakatlar rejasi ishlab chiqilishi lozim. Ushbu reja Xodimlarning lavozim tavsiflari, bo‘linmalar to‘g‘risidagi nizom, tashkilotning shartnomaviy

(kontrakt) majburiyatlari axborot xavfsizligini ta’minlash uchun mas’uliyat va majburiyatlarni o‘z ichiga olishi kerak. Tashkilotning barcha xodimlarini tasdiqlangan siyosat talablari va qoidalari bilan tanishtirish, shuningdek, axborot xavfsizligi masalalari bo‘yicha muntazam tushuntirish tadbirlarini o‘tkazish tartibini ta’minlash kerak. Agar siyosat talablari tashkilotdan tashqariga chiqsa, axborot xavfsizligi talablari uchinchi tomon tashkilotlari bilan shartnoma majburiyatlariga kiritilishi kerak.

Axborotni muhofaza qilishning samaradorligi unug o‘z vaqtidaligi, faolligi, uzluksizligi va kompleksligi bilan belgilanadi. Himoya tadbirini kompleks tarzda o‘tkazish axborot tarqab ketishi mumkin bo‘lganxavfli kanallarni yo‘q qilishni ta’minlaydi.Vaholanki, birgina ochiq qolgan axborotning tarqab ketish kanali butun himoya tizimining samaradorligini keskin kamaytirib yuboradi.

Axborot hisoblash tizimlarida axborot xavfsizligini ta’minlash nuqtai nazaridan o‘zaro bog‘liq bo‘lgan uchta tashkil etuvchi ya’ni axborot; texnik va dasturiy vositalar; xizmat ko‘rsatuvchi personal va foydala-nuvchilarga e’tibor qaratiladi. Axborotni muhofaza qilish tamoillarini uch guruhga bo‘lish mumkin: Huquqiy, tashkiliy hamda texnik razvedkadan himoyanishda va hisoblash texnikasi axborotga ishlov berishda axborotni muho-faza qilishdan foydalanish. Axborotni muhofaza qilish tizimlaridan foydalanish amaliyoti shuni ko‘rsatmoqdaki, faqatgina kompleks axborotni muhofaza qilish tizimlari samarali bo‘lishi mumkin.

Foydalanilgan adabiyotlar

1. Vishnevskiy V.M. – Kompyuter tarmoqlarini qurishning nazariy asoslari – M.: “ Texnosfera ”, 2020. – 512 b .
2. Olifer V.G., Olifer N.A. – Kompyuter tarmoqlari – Sankt-Peterburg : “ Pyotr”, 2018 yil – 944 b.
3. Shangin V.F. – Kompyuter tizimlari va tarmoqlarida axborotni himoya qilish – M.: “DMK Press”, 2020. – 593 b .
4. Tanenbaum E. Kompyuter tarmoqlari. 5-nashr. - Sankt-Peterburg: "Peter", 2019. – 960 b .
5. Tonievich A. – Kompyuter tarmoqlari – M.: “ Aserfan ”, 2018. – 235 b .
6. Stallings V. Kompyuter tarmoqlari, protokollari va internet texnologiyalari - SP b.: "BHV-Peterburg", 2020. - 832 b.

Internet resuslar:

1.https://e-library.namdu.uz

2.http://tatumarkaz.uz

3.https://uz.m.wikipedia.org

4.https://www.ziyouz.com

5.https://allbest.ru

6.https://infourok.ru