AXBOROT XAVFSIZLIGI QOIDALARI

Respublika O'rta Tibbiyot Va Farmatsevt Xodimlar Malakasini Oshirish Va Ixtisoslashtirish Markazi Termiz Filiali Axborot Texnologiyasi Fani O'qituvchisi
Daminov Husniddin Gulmat O'g'li
Axatova Sarvinoz Muminovna

Annotatsiya: *Axborot tushunchasi va undan tog'ri foydalanish*
Kalit so'zi: *Axborot texnologiyasi, ma'lumotlar ombori, xavfsizlik choralari*.

Axborot xavfsizligi (inglizcha: Information Security, shuningdek, inglizcha: InfoSec) — axborotni ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o'zgartirish, tadqiq qilish, yozib olish yoki yo'q qilishning oldini olish amaliyotidir. Ushbu universal kontseptsiya ma'lumotlar qanday shaklda bo'lishidan qat'iy nazar (masalan, elektron yoki, jismoniy) amal qiladi. Axborot xavfsizligini ta'minlashning asosiy maqsadi ma'lumotlarning konfidensialligi, yaxlitligi va mavjudligini muvozanatli, qo'llashning maqsadga muvofiqligini hisobga olgan holda va tashkilot faoliyatiga hech qanday zarar yetkazmasdan himoya qilishdir. Bunga, birinchi navbatda, asosiy vositalar va nomoddiy aktivlar, tahdid manbalari, zaifliklar, potensial ta'sirlar va mavjud xavflarni boshqarish imkoniyatlarini aniqlaydigan ko'p bosqichli xavflarni boshqarish jarayoni orqali erishiladi. Bu jarayon xavflarni boshqarish rejasining samaradorligini baholash bilan birga olib boriladi.

Ushbu faoliyatni standartlashtirish maqsadida ilmiy va kasbiy hamjamiyatlar texnik axborot xavfsizligi choralari, yuridik javobgarlik, shuningdek, foydalanuvchi va ma'murlarni tayyorlash standartlari sohasida asosiy metodologiya, siyosat va tarmoq standartlarini ishlab chiqishga qaratilgan doimiy hamkorlik asosida ish olib boradi. Ushbu standartlashtirishga asosan ma'lumotlarga kirish, qayta ishlash, saqlash va uzatishni tartibga soluvchi keng ko'lamli qonunlar va qoidalar ta'sir ko'rsatadi. Biroq, tashkilotda agar doimiy takomillashtirish madaniyati to'g'ri shakllantirilmagan bo'lsa, har qanday standartlar va metodologiyalarni joriy etish yuzaki ta'sir ko'rsatishi mumkin

Umumiy ma'lumot

Axborot xavfsizligining markazida axborotni himoya qilish faoliyati — uning maxfiyligi, mavjudligi va yaxlitligini ta'minlash, shuningdek, tanqidiy vaziyatda har qanday murosaga yo'l qo'ymaslik masalasi yotadi . Bunday holatlarga tabiiy, texnogen va ijtimoiy ofatlar, kompyuterning ishdan chiqishi, jismoniy o'g'irlik va boshqalar kiradi. Dunyodagi aksariyat tashkilotlarning ish jarayonlari hanuz qog'oz asosidagi xujjatlarga asoslangan, bo'lib, tegishli axborot xavfsizligi choralarini talab qilsa-da, korxonalarda raqamli texnologiyalarni joriy etish bo'yicha tashabbuslar soni barqaror o'sib bormoqda . Bu esa axborotni himoya qilish uchun axborot texnologiyalari (IT) xavfsizligi bo'yicha mutaxassislarni jalb qilishni talab qiladi. Ushbu mutaxassislar axborot xavfsizligi texnologiyasini (ko'p hollarda kompyuter tizimlarining bir turini) ta'minlaydi. Bu kontekstda kompyuter nafaqat maishiy

shaxsiy kompyuterni, balki har qanday murakkablik va maqsadli raqamli qurilmalar, ya'ni elektron kalkulyatorlar va maishiy texnika kabi ibtidoiy va izolyatsiya qilinganlardan tortib, sanoat boshqaruv tizimlari va kompyuter tarmoqlari orqali ulangan superkompyuterlargacha bo'lgan raqamli qurilmalarni anglatadi. Yirik korxona va tashkilotlar o'z bizneslari uchun axborotning hayotiy ahamiyati va qiymati tufayli, qoida tariqasida, o'z xodimlariga axborot xavfsizligi bo'yicha mutaxassislarni yollaydilar. Ularning vazifasi barcha texnologiyalarni maxfiy ma'lumotlarni o'g'irlash yoki tashkilotning ichki tizimlarini nazorat qilishga qaratilgan zararli kiberhujumlardan himoya qilishdir.

Axborot xavfsizligi bandlik sohasi sifatida so'nggi yillarda sezilarli darajada rivojlandi va o'sdi. U tarmoq va tegishli infratuzilma xavfsizligi, dasturiy ta'minot va ma'lumotlar bazasini himoya qilish, axborot tizimlari auditi, biznesning uzluksizligini rejalashtirish, elektron yozuvlarni aniqlash va kompyuter kriminalistikasi kabi ko'plab professional ixtisosliklarni yaratdi. Axborot xavfsizligi bo'yicha mutaxassislar mehnat bozorida yuksak barqaror bandlikka va yuqori talabga ega. Bir qator tashkilotlar (ISC) tomonidan olib borilgan keng ko'lamli tadqiqotlar natijasida ma'lum bo'lishicha, 2017-yilda axborot xavfsizligi sohasi rahbarlarining 66 % o'z bo'limlarida ishchi kuchining keskin yetishmasligini tan olishgan va 2022-yilga kelib bu sohada mutaxassislarning tanqisligi darajasi butun dunyoda 1 800 000 kishini tashkil etishini taxmin qilgan

Tahdidlar va xavfsizlik choralari

Axborot xavfsizligiga tahdidlar turli shakllarda bo'lishi mumkin. 2018-yil uchun eng jiddiy tahdidlar „xizmat ko'rsatish usulidagi jinoyatlar" (inglizcha: Crime-as-a-Service), Internet mahsulotlari, ta'minot zanjirlari va tartibga solish talablarining murakkabligi bilan bog'liq bo'lgan tahdidlar bo'lgan [10]. „Xizmat ko'rsatish usulidagi jinoyatlar" yirik jinoiy hamjamiyatlar uchun darknet bozorida jinoiy xizmatlar paketini yangi paydo bo'lgan kiberjinoyatchilarga arzon narxlarda taqdim etishning bir namunasidir. Bu yuqori texnik murakkablik yoki yuqori narx tufayli ilgari erishib bo'lmagan xakerlik hujumlarini amalga oshirish imkonini beradi. Bu esa kiberjinoyatni ommaviy hodisaga aylantiradi. Ko'pgina tashkilotlar Internet mahsulotlarini faol tatbiq qilmoqdalar. Bu qurilmalar ko'pincha xavfsizlik talablarisiz ishlab chiqilganligi bois, kiberhujumlar uchun qo'shimcha imkoniyatlar yaratadi. Bundan tashqari, internet xizmatlarining jadal rivojlanishi va murakkablashuvi uning shaffofligini pasaytiradi, bu esa noaniq belgilangan huquqiy qoidalar va shartlar bilan birgalikda tashkilotlarga qurilmalar tomonidan to'plangan mijozlarning shaxsiy ma'lumotlaridan o'z ixtiyoriga ko'ra, ular bilmagan holda foydalanish imkonini beradi. Bundan tashqari, tashkilotlarning o'zlari IoT qurilmalari tomonidan to'plangan ma'lumotlarning qaysi biri tashqariga uzatilishini kuzatishi mushkul masaladir. Ta'minot zanjirlariga tahdid shundaki, tashkilotlar o'zlarining yetkazib beruvchilari bilan turli xil qimmatli va nozik ma'lumotlarni almashishadi, natijada ular ustidan bevosita nazorat yo'qoladi. Shunday qilib, ushbu ma'lumotlarning maxfiyligi, yaxlitligi yoki mavjudligini buzish xavfi sezilarli darajada oshadi. Bugungi kunda regulyatorlarning tobora ko'payib borayotgan yangi talablari tashkilotlarning hayotiy axborot aktivlarini boshqarishni sezilarli

darajada murakkablashtirmoqda. Masalan, 2018-yilda Evropa Ittifoqida qabul qilingan „Umumiy ma’lumotlarni himoya qilish qoidalari“ (inglizcha: General Data Protection Regulation, GDPR) har qanday tashkilotdan istalgan vaqtda o‘z faoliyati yoki ta’minot zanjirining istalgan qismida joylashtirilgan shaxsiy ma’lumotlarning mazmuni, ularni qayta ishlash usullari, saqlanish va himoyalanish tartibi va qanday maqsadlar uchun xizmat qilishini ko‘rsatishni talab qiladi. Bundan tashqari, ushbu ma’lumot nafaqat vakolatli organlar tomonidan tekshirish paytida, balki ushbu ma’lumotlar egasining birinchi talabiga binoan ham taqdim etilishi lozim. Bunday muvofiqlikka rioya qilish muhim byudjet mablag‘lari va resurslarini tashkilotning boshqa axborot xavfsizligi vazifalaridan chetlashtirishni talab qiladi. Shaxsiy ma’lumotlarni qayta ishlashni soddalashtirish uzoq muddatli istiqbolda axborot xavfsizligini yaxshilashni nazarda tutsa ham, qisqa muddatda tashkilotning xatarlari sezilarli darajada oshadi .

Aksariyat odamlar u yoki bu tarzda axborot xavfsizligi tahdidlariga duchor bo‘lishadi. Masalan, ular zararli dasturlar (viruslar va kompyuter qurti, troya oti(kompyuter virusi) va firibgarlik dasturlari), fishing yoki identifikatorni o‘g‘irlash qurboni bo‘lishadi. Fishing (inglizcha: Phishing) — maxfiy ma’lumotlarni (masalan, hisob, parol yoki kredit karta ma’lumotlari) olishga qaratilgan firibgarlik harakatlaridir. Odatda, ular internet foydalanuvchisini har qanday tashkilotning (bank, internet-do‘kon, ijtimoiy tarmoq va h.k.) asl veb-saytidan ajratib bo‘lmaydigan soxta veb-saytga jalb qilishga harakat qiladilar . Qoida tariqasida, bunday urinishlar tashkilot nomidan soxta veb-saytlarga havolalarni o‘z ichiga olgan soxta elektron pochta xabarlarini ommaviy yuborish orqali amalga oshiriladi. Foydalanuvchi brauzerda bunday havolani ochib, o‘z hisob ma’lumotlarini kiritib firibgarlarning o‘ljasiga aylanadi . 1964-yilda ingliz tiliga Andoza:Tr kiritilgan bo‘lib, unda kimningdir shaxsiy ma’lumotlari (masalan, ko‘pincha fishing yo‘li bilan olingan ism, bank hisobi yoki kredit karta raqami) firibgarlik va boshqa jinoyatlarni sodir etishda foydalaniladi. Jinoyatchilar nomidan noqonuniy moliyaviy imtiyozlar, qarz olgan yoki boshqa jinoyatlarni sodir etgan shaxs ko‘pincha ayblanuvchining o‘zi bo‘lib qoladi va bu uning uchun jiddiy moliyaviy va huquqiy oqibatlarga olib kelishi mumkin. Axborot xavfsizligi shaxsiy hayotga bevosita ta’sir qiladi va bu holat turli madaniyatlarda turlicha ta’riflanishi mumkin.

Hukumatlar, harbiylar, korporatsiyalar, moliya institutlari, tibbiyot muassasalari va xususiy korxonalar o‘z xodimlari, mijozlari, mahsulotlari, tadqiqotlari va moliyaviy natijalari haqida doimiy ravishda katta miqdordagi maxfiy ma’lumotlarni to‘playdi. Agar bunday ma’lumotlar raqobatchilar yoki kiberjinoyatchilar qo‘liga tushib qolsa, bu tashkilot va uning mijozlari uchun keng qamrovli huquqiy oqibatlarga, tuzatib bo‘lmas moliyaviy va ayanchli yo‘qotishlarga olib kelishi mumkin. Biznes nuqtai nazaridan, axborot xavfsizligi xarajatlarga nisbatan muvozanatli bo‘lishi kerak. Gordon-Lob[en] iqtisodiy modeli bu muammoni hal qilishning matematik apparatni tavsiflaydi Unga ko‘ra axborot xavfsizligi tahdidlari yoki axborot xavflariga qarshi kurashishning asosiy usullari quyidagilardan iborat:

- kamaytirish — zaifliklarni bartaraf etish va tahdidlarning oldini olish uchun xavfsizlik va qarshi choralarni amalga oshirish;

•uzatish — tahdidlarni amalga oshirish bilan bog‘liq xarajatlarni uchinchi shaxslar: sug‘urta yoki autsorsing kompaniyalariga o‘tkazish;

•qabul qilish — xavfsizlik choralarini amalga oshirish xarajatlari tahdidni amalga oshirishdan mumkin bo‘lgan zarardan oshib ketgan taqdirda moliyaviy zaxiralarni shakllantirish;

•voz kechish — haddan tashqari xavfli faoliyatdan voz kechish

Asosiy ta’riflar

Himoya qilinadigan axborot — normativ-huquqiy hujjatlar talablariga yoki axborot egasi tomonidan belgilangan talablarga muvofiq muhofaza qilinishi kerak bo‘lgan axborotdir.

Axborot egasi — axborotni mustaqil ravishda yaratgan qonun yoki shartnoma asosida har qanday belgilar bilan aniqlangan ma’lumotlarga kirishga ruxsat berish yoki cheklash huquqini olgan shaxs. Axborot egalari quyidagilar bo‘lishi mumkin: davlat, yuridik shaxs, jismoniy shaxslar guruhi, alohida jismoniy shaxs.

Axborot xavfsizligi — axborot xavfsizligi holati, bunda uning maxfiyligi, yaxlitligi va mavjudligi ta’minlanadi.

Axborot xavfsizligini tashkil etish — axborot xavfsizligiga tahdidlarni aniqlash, axborotni himoya qilish bo‘yicha chora-tadbirlarni rejalashtirish, amalga oshirish va axborotni muhofaza qilish holatini kuzatishga qaratilgan harakatlar majmui

Axborot xavfsizligi tizimi — axborot xavfsizligi talablariga muvofiq tashkil etilgan va faoliyat yurituvchi organlar va (yoki) ijrochilar, ular tomonidan qo‘llaniladigan axborotni muhofaza qilish texnologiyalari, shuningdek axborotni muhofaza qilish ob’ektlari majmui

Tashkilotning axborot xavfsizligi siyosati — bu tashkilot faoliyatini tartibga soluvchi hujjatlashtirilgan axborot xavfsizligi siyosatlari, protseduralari, amaliyotlari yoki yo‘riqnomalari to‘plam

Turli manbalarda „axborot xavfsizligi“ tushunchasi

Quyida turli manbalardan olingan „axborot xavfsizligi“ atamasining ta’riflari keltirilgan:

•Axborotning maxfiyligi, yaxlitligi va mavjudligini saqlash. Eslatma: Haqiqiylik, javobgarlik, rad etmaslik (inglizcha: non-repudiation) va ishonchlilik kabi boshqa xususiyatlar ham bu qatorga kiritilishi mumkin .

•Maxfiylik, yaxlitlik va mavjudlikni ta’minlash maqsadida axborot va axborot tizimlarini ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o‘zgartirish yoki yo‘q qilishdan himoya qilish .

•Korxonada axborotni ruxsatsiz foydalanuvchilarga oshkor qilishdan (maxfiylik), noqonuniy o‘zgartirishdan (yaxlitlik) va zarur bo‘lganda mavjud bo‘lmasligidan (mavjudligi) himoya qilishni ta’minlash.

•Tashkilotning intellektual mulkini himoya qilish jarayoni .

•Xatarlarni boshqarish fanlaridan biri, uning vazifasi biznes uchun axborot tavakkalchiligi xarajatlarini boshqarishdir

•Axborot risklari tegishli nazorat va boshqaruv choralari bilan muvozanatlanganligiga asosli ishonch.

•Axborotni himoya qilish, axborotni shaxslarga ruxsatsiz oshkor qilish xavfini minimallashtirish

•Axborotni qayerda joylashgan bo‘lishidan qat’iy nazar (tashkilot perimetri ichida ham, tashqarisida ham) tahdidlardan himoya qilish uchun turli xil xavfsizlik mexanizmlari (texnik, tashkiliy, insonga yo‘naltirilgan, huquqiy)ni ishlab chiqish va amalga oshirishga qaratilgan ko‘p tarmoqli tadqiqot va kasbiy faoliyat sohasi va shunga mos ravishda axborot yaratiladigan, qayta ishlanadigan, saqlanadigan, uzatiladigan va yo‘q qilinadigan axborot tizimlari. Xavfsizlik maqsadlari ro‘yxati maxfiylik, yaxlitlik, mavjudlik, maxfiylik, haqiqiylik va asoslilik, rad etmaslik, javobgarlik va tekshiriluvchanlikni o‘z ichiga olishi mumkin

•Davlat xavfsizligi uchun mas’ul bo‘lgan davlat organlari tomonidan paydo bo‘ladigan, ta’sir etuvchi tahdidlar va ushbu tahdidlarga qarshi kurashning muvaffaqiyati o‘rtasidagi muvozanat jarayoni

Asosiy tamoyillar

1975-yilda Jerri Zalser va Maykl Shreder o‘zlarining „Kompyuter tizimlarida axborot xavfsizligi“ nomli maqolasida birinchi bo‘lib xavfsizlikni buzishni uchta asosiy toifaga ajratishni taklif qilishgan. Bular ma’lumotlarni ruxsatsiz oshkor qilish (inglizcha: unauthorized information release), ma’lumotni ruxsatsiz o‘zgartirish (inglizcha: Unauthorized information modification) va ma’lumotlarga kirishni ruxsatsiz rad etish (inglizcha: Unauthorized denial of use). Keyinchalik, bu toifalar quyidagi qisqa nomlar va standartlashtirilgan ta’riflarni olgan:

Confidentiality ing. „maxfiylik“ - ruxsatsiz shaxslar, sub’ektlar yoki jarayonlar uchun kirish mumkin bo‘lmagan yoki yopiq bo‘lgan ma’lumotlarning xususiyat

Integrity ing. „yaxlitlik“ - aktivlarning to‘g‘riligi va to‘liqligini saqlash xususiyat;

Availability ing. „mavjudlik“ - bu huquqqa ega bo‘lgan vakolatli sub’ektning iltimosiga binoan mavjud bo‘lishi va foydalanishga tayyor bo‘lishi kerak bo‘lgan ma’lumotlar mulki

Axborot xavfsizligining ushbu uchta asosiy tamoyillari birgalikda CIA triadasi deb ataladi.

1992-yilda IHTT (Iqtisodiy hamkorlik va taraqqiyot tashkiloti) o‘zining xabardorlik, mas’uliyat, qarshilik, axloq, demokratiya, xavflarni baholash, xavfsizlikni loyihalash va amalga oshirish, xavfsizlikni boshqarish, qayta ko‘rib chiqish kabi to‘qqiz tamoyildan iborat axborot xavfsizligi modelini nashr etdi. 1996-yilda IHTTning 1992-yildagi nashriga asoslanib, Amerika Milliy Standartlar va Texnologiyalar Instituti (NIST) kompyuter xavfsizligi haqida quyidagi sakkiz tamoyilni targ‘ib qilgan. Unga ko‘ra axborot xavfsizligi: „tashkilot missiyasini qo‘llab-quvvatlaydi“, „sog‘lom menejmentning ajralmas qismidir“, „xarajat jihatidan samarali bo‘lishi kerak“, „har tomonlama va kompleks yondashuvni talab qiladi“, „ijtimoiy omillar bilan cheklangan“, „vaqti-vaqti bilan ko‘rib chiqilishi talab etiladi“, „kompyuter xavfsizligi bo‘yicha majburiyatlar va mas’uliyatlar aniq ifodalangan bo‘lishi lozim“ va „tizim egalari o‘z tashkilotidan tashqari xavfsizlik uchun javobgardir’’Ushbu modelga asoslanib,

2004-yilda NIST 33 ta axborot xavfsizligi muhandisligi dizayn tamoyillarini nashr etgan. Ularning har biri uchun amaliy ko‘rsatmalar va tavsiyalar ishlab chiqilgan bo‘lib, ular doimiy ravishda nazorat qilinadi va yangilanadi

1998-yilda Donn Parker klassik Markaziy razvedka boshqarmasi triadasini egalik yoki nazorat (inglizcha: Possession or Control), haqiqiylik (inglizcha: Authenticity) va foydalilik (inglizcha: Utility) kabi yana uch jihat bilan to‘ldirdi Parker geksadi (ing. hexad – ,,oltita elementdan iborat guruh”) deb ataluvchi ushbu modelning afzalliklari, axborot xavfsizligi mutaxassislari o‘rtasida muhokama mavzusi hisoblanadi

Ayni paytda, professional hamjamiyatda Markaziy razvedka boshqarmasi CIA triadasining tez rivojlanayotgan texnologiyalar va biznes talablariga qanchalik mos kelishi haqida munozaralar davom etmoqda. Ushbu muhokamalar natijasida xavfsizlik va shaxsiy daxlsizlik o‘rtasidagi munosabatlarni o‘rnatish, qo‘shimcha tamoyillarni qabul qilish zarurligi to‘g‘risida tavsiyalar berildi

Ulardan ayrimlari allaqachon Xalqaro standartlashtirish tashkiloti (ISO) standartlariga kiritilgan:

•haqqoniylik (inglizcha: authenticity) – ob’ekt yoki resursning e’lon qilingan bilan bir xilligini kafolatlaydigan xususiyat;

•javobgarlik[en] (inglizcha: accountability) – sub’ektning o‘z harakatlari va qarorlari uchun javobgarligi;

•rad etishning imkonsizligi (inglizcha: non-repudiation) — sodir bo‘lgan voqea yoki harakatni va ularning sub’ektlarini ushbu hodisa yoki harakatni va u bilan bog‘liq bo‘lgan sub’ektlarni shubha ostiga qo‘ymaslik uchun tasdiqlash qobiliyati;

•ishonchlilik (inglizcha: reliability) – bu mo‘ljallangan xatti-harakatlar va natijalarga muvofiqlik xususiyatidir.

Hulosa: Axborotning maxfiyligiga minimal zarur xabardorlik (inglizcha: need-to-know) tamoyiliga asoslanib, unga eng kam imtiyozlar bilan ruxsat berish orqali erishiladi. Boshqacha qilib aytganda, vakolatli shaxs faqat yuqorida aytib o‘tilgan shaxsiy daxlsizlikka qarshi jinoyatlar, masalan, shaxsni o‘g‘irlash, shaxsiy hayotning buzilishi kabi o‘z xizmat vazifalarini bajarishi uchun zarur bo‘lgan ma’lumotlarga ega bo‘lishi talab etiladi. Maxfiylikni ta’minlashning eng muhim chora-tadbirlaridan biri ma’lumotlarni qat’iy maxfiy yoki ommaviy, shuningdek, ichki foydalanish uchun mo‘ljallangan ma’lumotlarni tasniflash imkonini beradi. Axborotni shifrlash konfidensiallikni ta’minlash vositalaridan birining tipik namunasidir

FOYDALANILGAN ADABIYOTLAR:

O'n ikki Qaysarning hayoti. M.: nashriyot "Fan", 1964 yil.

Singx, Saymon. Shifr kitob. Shifrlarning maxfiy tarixi va ularni dekodlash. M.: "AST" nashri, 2009. ISBN 5-17-038477-7.

"Qora shkaflar". Moskva: Yangi adabiy sharh, 2015. ISBN 978-5-4448-0392-9.

Jelnikov V.: Papirusdan kompyuterga kriptografiya

Anin B.Yu.: Elektron josuslik

Kriptografiya rivojlanishining qisqacha tarixiy tavsifi. Moskva universiteti va Rossiyada kriptografiyaning rivojlanishi, Moskva davlat universiteti, 2002 yil 17-18 oktyabr, 2002 yil.

Rossiyada kriptografiya tarixi haqida. Amaliy diskret matematika, 2012 yil. "Maxfiylik, yaxlitlik, mavjudlik" triadasi: u qayerdan keladi? SecurityLab.ru, 2012