Emro Science and Education
Open-access scientific journal
Journal homepage: https://journal.emro.uz
OPEN ACCESS

CONFERENCE PAPER OPEN ACCESS

Vol. 1 No. 2 (2024) · “Raqamli iqtisodiyot sharoitida moliyaning dolzarb muammolari, yechimlari va istiqbollari” mavzusidagi ilmiy-amaliy...

enterprise will bring positive results to the enterprise. Because these theories are being used in practice in enterprises worldwide. In our opinion, the application of these theories, enriched with additional modern factors, will improve the system of working with personnel in the digital economy. For example, according to A. Maslow's pyramid of needs, in the enterprise, with the help of programs working with MS Access or other databases, an appropriate database is created based on the existing needs of employees, and their needs are controlled based on this.

The HR (human resource) department updates the database as a result of daily studies. Based on the weekly analysis of the database, the manager develops and implements a motivational system for effective personnel management. Currently, there are effective systems of motivational management of personnel based on world experience, but we need to develop a motivational system suitable for the conditions of Uzbekistan, having studied foreign experience. Because every nation has its own customs, nature, interests, and beliefs. Taking these factors into account, it is necessary to enrich the above theories and introduce improved systems to enterprises.

Associate Professor, scientific supervisor M. Akhunov,

List of used literature:

1. Taylor F.U. Nauchnaya organization is working. - M.: NKPS - Transpechat, 1924; Taylor and Taylorism: technique.
2. Travin V.V., Magura M.I., Kurbatova M.B. Motivational management. - S. 4345; Classical management. Encyclopedia... - S. 473-479.
3. Maslow A. Self-actualization. // Psychology lichnosti: texty. - M.: izd-vo Moskovskogo universiteta, 1982. - S. 108-117.
4. Greenberg D., Byron D. Organizational behavior: theory and practice. - M.: Vershina, 2004. - S. 299.
5. Travin V.V. Management personnel of the enterprise: Ucheb. - practice. posobie.- M.: Delo, 2003.c 135. Macroeconomic stability

AXBOROT XAVFSIZLIGI VA UNI SHAKLLANTIRISH JARAYONI

Yusupov M.T.
“Mutaxassislik fanlari” kafedrasi dotsenti
Xabibullayeva Feruzabonu
“Iqtisodiyot” yo’nalishi birinchi kurs talabasi
feruzabonuxabibullayeva30@gmail.com

Annotatsiya

Hozirgi kunda axborot va unga nisbatan tashqi, turli ko’rinishdagi ta’sirlarni oldini olish shu kunning dolzarb masalalaridan biridir. Ushbu muammoni hal qilish

Published: 28.03.2024
Cite this article: Yusupov M.T., Xabibullayeva Feruzabonu (2024). Axborot xavfsizligi va uni shakllantirish jarayoni. Emro Science and Education, 1(2). https://journal.emro.uz/public/maqola/257
© 2024 The Author(s). Published by Emro Science and Education. This is an open access article.

maqsadida dunyo olimlari va mutaxasislari tomonidan turli tadbirlar tashkil etilmmoqda. Maqolamizda axborot xavfsizligiga nisbatan taxdidlar va ulardan ximoyalanish usullari haqida fikr bildiramiz.

Kalit so’zlar: Axborot xavfsizligi, axborot xavsizligiga bo’lgan taxdidlar va axborot muhofazasi.

Biz bilamizki, hozirgi kunda hayotimizni axborot texnalogiyalarisiz tassavur eta olmaymiz va albatta dunyoning axborot texnalogiyalari kirib kelmagan davlatni o’zi bo’lmasa kerak.

Bizga ma’lumki 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 amaliyoti hisoblanadi. 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 va qo‘llashning maqsadga muvofiqligini hisobga olgan holda va tashkilot faoliyatiga hech qanday zarar yetkazmasdan himoya qilishdan iborat. 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.

Hozirgi kunda ushbu faoliyatni standartlashtirish maqsadida ilmiy va kasbiy hamjamiyatlar texnik axborot xavfsizligi choralari, yuridik javobgarlik va shuningdek, foydalanuvchi va ma’murlarni tayyorlash standartlari sohasida asosiy metodologiya, siyosat va tarmoq standartlarini ishlab chiqishga qaratilgan doimiy hamkorlik asosida ish olib borilmoqda. Ushbu standartlashtirishga asosan ma’lumotlarga kirish, qayta ishlash, saqlash va uzatishni tartibga soluvchi keng ko‘lamli qonunlar va qoidalar ta’sir ko‘rsatilyapti. 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. Shuningdek axborot bor joyda unga bo’lgan tahdid ham bo’ladi va axborot xavfsizligiga bo’lgan 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 edi . „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 hakerlik 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 esa mushkul masaladir. Ta’minot zanjirlariga tahdid shundaki, tashkilotlar o‘zlarining yetkazib beruvchilari bilan turli xil qimmatli va nozik ma’lumotlarni almashishadi va 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 Yevropa Ittifoqida qabul qilingan „Umumiy ma’lumotlarni himoya qilish qoidalari“ har qanday tashkilotdan istalgan vaqtda o‘z faoliyati yoki ta’minot zanjirining istalgan qismida joylashtirilgan shaxsiy ma’lumotlarning mazmuni, ularni qayta ishlash usullari, saq lanish 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 muhimdir. 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.

Bugungi kunda aksariyat odamlar u yoki bu kabi axborot xavfsizligi tahdidlariga duchor bo‘lishmoqda. Masalan, ular zararli dasturlar (viruslar va kompyuter qurti, troya oti(kompyuter virusi) va firibgarlik dasturlari), fishing yoki identifikatorni o‘g‘irlash qurboni bo‘lishyapti. Bunda agar biz “Fishing” haqida aytadigan bo’lsak bu (inglizcha: *Phishing*) — maxfiy ma’lumotlarni (masalan, hisob, parol yoki kredit karta ma’lumotlari) olishga qaratilgan firibgarlik harakati hisoblanadi. 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 .Bu 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.

Bu axborotga bo’lgan taxdidning bir turi holos, agar biz bu to’g’risida izlanishlar olib borsak bundan tahdidlarning ko’piga duch kelishimiz mumkindir.

Albatta tahdid bo’lgan joyda, unga nisbatan xavfsizlik choralari ko’riladi. Bizning mavzuyimizda bu axborot muhofazasi deb yuritiladi va bu keng ma’noda axborot xavfsizligiga bo’lgan tahdidni oldini olish va ularning asoratlarini yo’q qilishga qaratilgan tashkiliy ,huquqiy va texnik choralar kompleksini bildiradi. Axborotni muhofaza qilish bu axborotga bo’lgan salbiy ta’sir manbalarini hamda sabab va sharoitlarini aniqlash va bartaraf etish ma’nosini anglatadi.Bu manbalar esa axborot xavfsizligiga tahdidlarni tashkil etadi. Buning oldiini olish uchun bugungi kunda ko’plab chora tadbirlar ko’rilmoqda va bundan foydalanilmoqda.

Demak, biz aytishimiz mumkinki hozirgi kunimiz bevosita axborot texnalogiyalari bilan chambarchas bog’liqdir va bunda axborot xavfsizligini ham ro’li muhim hisoblanadi deya olamiz.

ADABIYOTLAR

1. Stewart, James Michael; Mike, Chapple; Darril, Gibson. *CISSP® Certified Information Systems Security Professional Study Guide*. Canada: Seventh Edition,John Wiley & Sons, Inc., 2015. ISBN 978-1-119-04271-6.
2. *Жизнь двенадцати цезарей*. M.: publisher «Наука», 1964.
3. Анин Б.Ю.: Радиоэлектронный шпионаж
4. Samonas, S.; Coss, D.. *The CIA Strikes Back Redefining Confidentiality, Integrity and Availability in Security*. Washington DC, USA: Information Institute Publishing, 2014

ISTE’MOLCHINING BOZORDAGI HARAKATI

Qurbonov Jasurbek Pozilovich
“Mutaxassislik fanlari” kafedrasi mudiri, i.f.f.d.
Maftuna Aliasqarovna Yigitaliyeva
Toshkent moliya instituti talabasi

Annotatsiya: Iste’molchilarning xatti-harakatlarini o’rganish, masalan, individual fazilatlarni rasmiy ravishda tekshiradi demografiya, shaxsiyat turmush tarzi va xulq-atvor o’zgaruvchilari. Ushbu tezisda bozordagi iste’molchilarning xatti-harakatlariga turli omillar, jumladan, psixologik, ijtimoiy va iqtisodiy jihatlar ta’sir qiladi, ular oxir-oqibatda xarid qilish qarorlari va iste’molchilarning xohish-istaklarini shakllantirish haqida so’z yuritilgan.