ISSN 2181-

BUXGALTERIYA MA’LUMOTLARINI XAVFSIZLIGINI TAMINLASHDA KIBERXAVFSIZLIK CHORALARI VA ULARNI BARTARAF ETISH USULLARI

Namangan davlat universiteti
Iqtisodiyot fakulteti
Buxgalteriya hisobi yo‘nalishi talabasi
Islomjonova Gulzoda Xayrulla qizi

Annotatsiya: Buxgalteriya ma'lumotlarini xavfsizligini ta'minlash kiberxavfsizlik sohasida muhim masala hisoblanadi. Buxgalteriya ma'lumotlari tashkilotning moliyaviy holatini, operatsion faoliyatini va strategik rejalashtirishini aks ettiradi. Ularning xavfsizligi nafaqat moliyaviy yo'qotishlarni oldini olish, balki tashkilotning obro'sini saqlash uchun ham zarurdir. Kiberxavfsizlik choralari va ularni bartaraf etish usullari buxgalteriya ma'lumotlarining xavfsizligini ta'minlashda muhim rol o'ynaydi. Ushbu maqolada buxgalteriya ma’lumotlarini xavfsizligini taminlashda kiberxavfsizlik choralari va ularni bartaraf etish usullari haqida ma'lumotlar berilgan.

Kalit so‘zlar: buxgalteriya, ma'lumotlar, kiberxavfsizlik, moliyaviy hisobotlar, daromadlar, hisobotlar, xarajatlar, moliyaviy yo'qotishlar.

Аннотация: Обеспечение безопасности данных бухгалтерского учета является важным вопросом в области кибербезопасности. Данные бухгалтерского учета отражают финансовое состояние, операционную деятельность и стратегическое планирование организации. Их безопасность необходима не только для предотвращения финансовых потерь, но и для сохранения репутации организации. Меры кибербезопасности и методы их устранения играют важную роль в обеспечении безопасности данных бухгалтерского учета. В данной статье представлена информация о мерах кибербезопасности и методах их устранения в обеспечении безопасности данных бухгалтерского учета.

Ключевые слова: бухгалтерский учет, данные, кибербезопасность, финансовая отчетность, доходы, отчеты, расходы, финансовые потери.

Abstract: Ensuring the security of accounting data is an important issue in the field of cybersecurity. Accounting data reflects the financial condition, operational activities and strategic planning of the organization. Their security is necessary not only to prevent financial losses, but also to preserve the reputation of the organization. Cybersecurity measures and methods for their elimination play an important role in ensuring the security of accounting data. This article provides information on cybersecurity measures and methods for their elimination in ensuring the security of accounting data.

Keywords: accounting, data, cybersecurity, financial statements, income, reports, expenses, financial losses.

KIRISH

Buxgalteriya, tashkilotlarning moliyaviy faoliyatini boshqarish va nazorat qilish jarayoni sifatida, har bir biznesning asosiy poydevorlaridan biridir. U moliyaviy ma'lumotlarni to'plash, qayd etish, tahlil qilish va hisobot berish orqali tashkilotning iqtisodiy holatini aks ettiradi. Buxgalteriya nafaqat moliyaviy hisobotlarni tayyorlashni, balki xarajatlar, daromadlar va aktivlar bilan bog'liq jarayonlarni boshqarishni ham o'z ichiga oladi. Buxgalteriya tizimi har bir tashkilotning muvaffaqiyatli faoliyat yuritishi uchun muhim ahamiyatga ega. U moliyaviy resurslarni samarali taqsimlash, xarajatlarni nazorat qilish va strategik qarorlar qabul qilishda yordam beradi. [1]

Buxgalteriya orqali tashkilotlar o'z moliyaviy holatini doimiy ravishda kuzatib borishlari va kerakli o'zgarishlarni amalga oshirishlari mumkin. Shuningdek, buxgalteriya qonuniy talablar va me'yorlarga rioya qilishni ta'minlaydi. Tashkilotlar moliyaviy hisobotlarni tayyorlashda va taqdim etishda aniq va shaffof bo'lishlari zarur. Bu esa investorlar, kredit beruvchilar va boshqa manfaatdor tomonlar uchun ishonchni oshiradi. Zamonaviy texnologiyalar yordamida buxgalteriya jarayonlari yanada samarali va tezkor amalga oshirilishi mumkin. Elektron buxgalteriya tizimlari va

dasturlari, ma'lumotlarni avtomatik tarzda qayd etish va tahlil qilish imkonini beradi, bu esa xatolarni kamaytiradi va ish jarayonlarini soddalashtiradi. Umuman olganda, buxgalteriya — bu tashkilotning moliyaviy barqarorligini ta'minlash va rivojlanish strategiyalarini ishlab chiqishda muhim rol o'ynaydigan jarayondir. Bu soha nafaqat moliyaviy ma'lumotlarni boshqarish, balki tashkilotning umumiy muvaffaqiyatiga hissa qo'shish uchun ham zarurdir.[2]

ADABIYOTLAR TAHLILI VA TADQIQOT METODOLOGIYASI

Kiberxavfsizlikning ahamiyatini tushunish uchun, avvalo, ma'lumotlarning qadrini bilish kerak. Har qanday tashkilot uchun ma'lumotlar — bu uning eng qimmatbaho aktivlaridan biridir. Buxgalteriya ma'lumotlari esa, moliyaviy hisobotlar, xarajatlar, daromadlar va boshqa muhim ko'rsatkichlarni o'z ichiga oladi. Agar bu ma'lumotlarga kiberhujumlar orqali kirish imkoniyati bo'lsa, bu nafaqat moliyaviy yo'qotishlarga olib kelishi, balki tashkilotning obro'siga ham zarar etkazishi mumkin. Shuning uchun, buxgalteriya ma'lumotlarini himoya qilish har bir tashkilotning ustuvor vazifalaridan biri bo'lishi kerak. Buxgalteriya ma'lumotlariga tahdidlar ko'plab shakllarda bo'lishi mumkin. Kiberhujumlar, ma'lumotlarni o'g'irlash, viruslar va zararli dasturlar, phishing hujumlari va boshqa kiberxavflar — bularning barchasi buxgalteriya ma'lumotlarining xavfsizligini tahdid ostiga qo'yadi. Shuningdek, ichki xatolar, xodimlarning beparvoligi va shaxsiy ma'lumotlarni noto'g'ri saqlash ham muhim xavflardir. Bu tahdidlar bilan kurashish uchun samarali strategiyalar ishlab chiqish zarur. Xavfsizlik choralarini amalga oshirishda birinchi navbatda, ma'lumotlarni shifrlash usulidan foydalanish muhimdir. Shifrlash ma'lumotlarni o'g'irlash holatida ham ularni tushunib bo'lmaydigan holga keltiradi. Bu, kiberhujumchilarning ma'lumotlarga kirishini qiyinlashtiradi. Shuningdek, ma'lumotlar saqlanadigan serverlar va tizimlar xavfsizligini ta'minlash uchun zamonaviy xavfsizlik devorlari va antivirus dasturlaridan foydalanish zarur. Ushbu dasturlar doimiy ravishda yangilanib turilishi va har qanday tahdidga qarshi himoya choralarini ko'rishi kerak.[3]

MUHOKAMA VA NATIJALAR

Xodimlarni kiberxavfsizlik bo'yicha o'qitish ham muhim ahamiyatga ega. Xodimlar kiberhujumlar va phishing hujumlari haqida ma'lumotga ega bo'lishlari, shuningdek, qanday qilib o'z ma'lumotlarini himoya qilishlari kerakligini bilishlari zarur. O'qitish jarayonida xavfsizlik protokollari, kuchli parollarni yaratish va ularni saqlash, shuningdek, shubhali havolalarga bosmaslik kabi qoidalar o'rgatilishi kerak. Xodimlar, shuningdek, ichki xavfsizlik siyosatiga amal qilishlari va har qanday shubhali faoliyat haqida xabar berishlari kerak. Ma'lumotlarni muntazam ravishda zaxiralash ham muhimdir. Zaxira nusxalari yaratish, ma'lumotlar yo'qolgan yoki buzilgan taqdirda ularni qayta tiklash imkonini beradi. Zaxira nusxalari xavfsiz joyda saqlanishi va ularga kirish faqat muayyan xodimlarga ruxsat etilishi kerak. Zaxira jarayonlari muntazam ravishda amalga oshirilishi va ularning samaradorligi sinovdan o'tkazilishi zarur. Shuningdek, xavfsizlikni ta'minlashda tizimlarni va dasturlarni muntazam ravishda yangilab turish muhimdir. Yangilanishlar ko'pincha xavfsizlikni oshirishga qaratilgan bo'lib, yangi tahdidlarga qarshi himoya qiladi. Tizimlar va dasturlarni yangilash, ularning zaif joylarini bartaraf etadi va kiberhujumchilarning imkoniyatlarini cheklaydi.[4]

Kiberxavfsizlik choralarini amalga oshirishda, tashkilotlar o'zlarining xavfsizlik siyosatlarini ishlab chiqishlari va amalga oshirishlari kerak. Ushbu siyosatlar kiberxavfsizlikning asosiy tamoyillarini, xodimlar uchun qoidalarni va xavfsizlik choralarini o'z ichiga olishi kerak. Shuningdek, tashkilotlar o'z xavfsizlik siyosatlarini muntazam ravishda qayta ko'rib chiqishlari va yangilanishlarga moslashtirishlari zarur. Xavfsizlik choralarini bartaraf etish usullari ham muhimdir. Agar kiberhujum sodir bo'lsa, tashkilotlar tezkor javob berish rejasini ishlab chiqishlari kerak. Bu reja, hujumni aniqlash, uning ta'sirini kamaytirish va ma'lumotlarni tiklash jarayonlarini o'z ichiga olishi kerak. Tezkor javob berish rejasi, xodimlar va rahbariyat o'rtasida o'zaro aloqa va hamkorlikni ta'minlaydi.[5]

Kiberxavfsizlik sohasida texnologiyalar rivojlanishi bilan birga, yangi tahdidlar ham paydo bo'ladi. Shuning uchun, tashkilotlar o'z xavfsizlik choralarini doimiy

ravishda yangilab turishlari va yangi texnologiyalarni qo'llashlari zarur. Masalan, sun'iy intellekt va mashinani o'rganish kiberxavfsizlikni kuchaytirish uchun samarali vositalar bo'lishi mumkin. Ushbu texnologiyalar, tahdidlarni oldindan aniqlash va ularni bartaraf etish jarayonlarini tezlashtirishga yordam beradi.[6]

XULOSA

Xulosa qilib aytganda, buxgalteriya ma'lumotlarini xavfsizligini ta'minlash kiberxavfsizlik sohasida muhim masala hisoblanadi. Samarali kiberxavfsizlik choralarini amalga oshirish va ularni bartaraf etish usullarini bilish, har bir tashkilot uchun zarurdir. Ma'lumotlarni shifrlash, xavfsizlik dasturlaridan foydalanish, xodimlarni o'qitish, zaxira nusxalarini yaratish va tizimlarni yangilash kabi choralar, buxgalteriya ma'lumotlarining xavfsizligini oshirishga yordam beradi. Kiberxavfsizlik siyosatlarini ishlab chiqish va tezkor javob berish rejalarini tayyorlash ham muhim ahamiyatga ega. Kiberxavfsizlik sohasidagi yangi texnologiyalarni qo'llash, tahdidlarni oldini olish va ularni bartaraf etish jarayonlarini samarali ravishda amalga oshirishga yordam beradi. Tashkilotlar o'z ma'lumotlarini himoya qilish uchun zarur choralarni ko'rish orqali, moliyaviy barqarorlikni ta'minlash va obro'sini saqlab qolishlari mumkin.

FOYDALANILGAN ADABIYOTLAR

1. Abdullayev, A. (2020). "Kiberxavfsizlik va axborot himoyasi." Toshkent: O'zbekiston Milliy Universiteti.
2. Ismoilov, D. (2021). "Buxgalteriya ma'lumotlarini himoya qilish usullari." Samarqand: Samarqand Davlat Universiteti.
3. Qodirov, S. (2019). "Axborot texnologiyalari va kiberxavfsizlik." Buxoro: Buxoro Davlat Universiteti.
4. Tursunov, F. (2022). "Ma'lumotlarni shifrlash va xavfsizlik." Nukus: Qoraqalpog'iston Davlat Universiteti.

5. Karimov, R. (2023). "Kiberhujumlar va ularga qarshi kurash usullari." Toshkent: O'zbekiston Respublikasi Axborot Texnologiyalari va Kommunikatsiyalarini Rivojlantirish Vazirligi.

6. Murodov, E. (2024). "Kiberxavfsizlik strategiyalari." Andijon: Andijon Davlat Universiteti.

7. Yuldashev, A. (2023). "Buxgalteriya va moliyaviy ma'lumotlarni himoya qilish." Farg'ona: Farg'ona Davlat Universiteti.

8. Mirzaev, O. (2022). "Axborot xavfsizligi va uning ahamiyati." Toshkent: O'zbekiston Respublikasi Iqtisodiyot va San'at Universiteti.

9. Sodiqov, B. (2021). "Kiberxavfsizlik: muammolar va yechimlar." Namangan: Namangan Davlat Universiteti.

10. Tashkentov, X. (2023). "Buxgalteriya tizimlarida xavfsizlik choralarini amalga oshirish." Qarshi: Qarshi Davlat Universiteti.