ISHLAB CHIQARISHDA AXBOROT XAVSIZLIGINI QO‘LLASHNI TADQIQ QILISH

Andijon mashinasozlik inistituti talabasi

Rustamova Dilnoza Rustam qizi

Email: dilnozarustamova4979@gmail.com

Andijon, O‘zbekiston.

Annotation. Research on the application of information security in production is crucial for protecting data, safeguarding assets, and ensuring business continuity. At the core of information security lies the activity of protecting information by ensuring its confidentiality, availability, and integrity, as well as avoiding any compromise in critical situations. Such situations include natural, technological, and social disasters, computer failures, physical theft, and others.

Аннотаци. Исследования по применению информационной безопасности в производстве имеют важное значение для защиты данных, обеспечения безопасности активов и непрерывности бизнеса. В основе информационной безопасности лежит деятельность по защите информации, обеспечивая её конфиденциальность, доступность и целостность, а также исключение любых компромиссов в критических ситуациях. К таким ситуациям относятся природные, техногенные и социальные катастрофы, сбои компьютеров, физическое похищение и другие.

Annotatsiya. Ishlab chiqarishda axborot xavfsizligini qo'llash bo'yicha tadqiqotlar ma'lumotlarni himoya qilish, aktivlarni himoya qilish va biznesning uzluksizligini ta'minlash uchun muhimdir. 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.

Key words: *cyber attack, NIST SP 800-53, ISO/IEC 27001.*

Ключевые слова: *кибератака, NIST SP 800-53, ISO/IEC 27001.*

Kalit so‘zlar: *Kiber hujum, NIST SP 800-53, ISO/IEC 27001.*

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 (IT) xavfsizligi bo‘yicha mutaxassislarni jalb qilishni talab qiladi. Ushbu mutaxassislar axborot xavfsizligi texnologiyasini (ko‘p hollarda bir turini) ta’minlaydi. Bu kontekstda 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 - bu tashkilotning axborotlarini, tizimlarini va infrastrukturani xavfsizligini ta'minlashga qaratilgan chora-tadbirlar yig'indisi. Uning asosiy maqsadlari quyidagilar:

- Maxfiylik (axborotlarga ruxsatsiz kirishni cheklash).
- Butunlik (axborotlarning to‘g‘riligini va to‘liq saqlanishini ta'minlash).
- Mavjudlik (axborot va tizimlardan foydalanish imkoniyatlarini ta'minlash).

Axborot xavfsizligi bo'yicha asosiy tahdidlar quyidagilardan iborat:

- ❖ Kiber hujumlar (masalan, fishing, ransomware, DDoS hujumlar).
- ❖ Ichki tahdidlar (xodimlarning ruxsatsiz harakatlari).
- ❖ Tizim nosozliklari va tabiiy ofatlar.

Axborot xavfsizligi bo‘yicha xalqaro va milliy standartlar

Axborot xavfsizligini ta'minlashda quyidagi xalqaro standartlar keng qo‘llaniladi:

- ➢ **ISO/IEC 27001**: Bu axborot xavfsizligi menejment tizimini tashkil qilish bo‘yicha xalqaro standart hisoblanadi. ISO/IEC 27001: Ushbu xalqaro standart axborot xavfsizligini boshqarish tizimini (AXBT) yaratish, joriy etish va qo'llab-quvvatlashga tizimli yondashuvni taqdim etadi.
- ➢ **NIST SP 800-53**: AQSh Milliy standartlar instituti tomonidan ishlab chiqilgan xavfsizlik va maxfiylik nazorati. NIST Cybersecurity Framework: Milliy Standartlar va Texnologiyalar Instituti (NIST) tashkilotlarning kiberxavfsizlik holatini yaxshilash uchun keng qabul qilingan asosni taqdim etadi. U xavflarni boshqarish strategiyalarini, nazorat mexanizmlarini va xavfsiz operatsiyalar uchun ko'rsatmalarni o'z ichiga oladi.

Axborot xavfsizligi bo'yicha investitsiyalar va sarf-harajatlar ham muhim ahamiyatga ega. Xavfsizlikka yetarli miqdorda mablag' ajratish tashkilotning uzoq muddatli barqarorligi uchun muhim. 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 yuksak barqaror bandlikka va yuqori talabga ega. Umumjahon axborot globallashuvi jarayonlari axborot-kommunikatsiya texnologiyalarini nafaqat mamlakatlar iqtisodiyoti va boshqa sohalariga joriy etish, balki axborot tizimlari xavfsizligini ta’minlashni ham taqozo etayotir. O‘zbekiston axborot va kommunikatsiya texnologiyalari sohasidagi xalqaro xavfsizlik tizimiga Markaziy Osiyoda birinchilardan bo‘lib qo‘shildi. Axborot xavfsizligini ta’minlash bo‘yicha Aloqa, axborotlashtirish va

telekommunikatsiya texnologiyalari davlat qo‘mitasi tomonidan quyidagi chora-tadbirlar amalga oshiriladi: ma’lumotlar uzatish, telekommunikatsiya tarmoqlari, teleradioefir hamda axborot tizimlarida axborot xavfsizligini ta’minlashni takomillashtirish va rivojlantirish bo‘yicha davlat siyosatini yuritish, davlat organlarining axborot tizimlari va resurslari axborot xavfsizligi siyosatini ishlab chiqish va amalga oshirishga ko‘maklashish, davlat axborot tizimlari va resurslarining axborot xavfsizligini ta’minlash yuzasidan monitoring natijalari to‘g‘risidagi statistik ma’lumotlarni O‘zbekiston Respublikasi Aloqa, axborotlashtirish va telekommunikatsiya texnologiyalari davlat qo‘mitasiga belgilangan tartibda taqdim etish, telekommunikatsiyalar tarmoqlarining operatorlari va provayderlari bilan hamkorlik qilish, davlat organlarining kompyuter va axborot texnologiyalaridan foydalanish sohasidagi qonun buzilishlarining oldini olish masalalari bo‘yicha birgalikdagi ishlarini tashkil etish va ularning faoliyatini muvofiqlashtirish bo’yicha ko’plab ishlar amalga oshirilyapti. Internetning milliy foydalanuvchilarini Internet tarmog‘i milliy segmentida axborot xavfsizligiga paydo bo‘layotgan tahdidlar to‘g‘risida o‘z vaqtida xabardor qilish, shuningdek axborotlarni muhofaza qilish bo‘yicha konsultatsiya xizmatlari ko‘rsatish, qonun buzuvchilarni tahlil qilish, identifikatsiyalashda, axborotlar makonidagi ruxsatsiz yoxud buzuvchi harakatlarni amalga oshirishda foydalaniladigan metodlar va vositalarni tahlil qilishda huquqni muhofaza qilish organlari bilan hamkorlik qilinadi.

Xulosa.

Internet tarmog‘i milliy segmentida axborot xavfsizligi hodisalarining oldini olish bo‘yicha o‘zaro amaliy ishlarni tashkil etish maqsadida axborot xavfsizligi sohasidagi xalqaro hamkorlikni rivojlantirish mumkin. Tashkilotlarda katta hajmdagi ma'lumotlarni saqlash jarayonida axborot xavfsizligini ta'minlashning muhimligi va usullari haqida muloqot qilinadi. Katta hajmdagi ma'lumotlar, tashkilotlar uchun juda muhim bo'lishi bilan birga, ularga o'tkan zarar ham katta bo'lishi mumkin.

O‘qituvchi: Yoqubjonov S.

FOYDALANILGAN ADABIYOTLAR:

1. Зокирова Т., Ибрагимов Э. Веб-технологиялар. Тошкент, ТДИУ, 2007 йил.

2. Зокирова Т., Мусаева Н. Интернет технологиялар. Тошкент, ТДИУ, 2007 йил. – 182 бет.

3. Машарипов М., Ибрагимов Э. Ахборот технологиялари. Тошкент, ТДИУ, 2007 йил. – 194 бет.

4. Информатика. Ахборот технологиялари. Укув кулланмаси. 1-2 кисмлар. Тузувчилар: М.М. Арипов, А.Б. Ахмедов, Х.З Икрамов. ТДТУ, Т, 2003

5. https://mitc.uz/uz/pages/info_security