ISSN 2181-3187

AXBOROT TEXNOLOGIYALARI SOHASIDA SODIR ETILAYOTGAN HUQUQBUZARLIKLARNI OLDINI OLISH CHORALARINI TAKOMILLASHTIRISH

Esonov Elbek Sayfulla o‘g‘li
Toshkent shahar IIBB Shayxontohur tumani IIO FMB
1-sonli IIB HPB profilaktika inspektori leytenant

Annotatsiya. Ushbu maqolada axborot texnologiyalari sohasidagi qoidabuzarliklarning oldini olish choralarini kuchaytirish zarurati ko'rib chiqilgan. Adabiyotlarni tahlil qilish orqali xavflarni kamaytirish va raqamli aktivlarni himoya qilish uchun turli strategiyalar, metodologiyalar va texnologiyalar tekshiriladi. Usullar bo'limi axborot texnologiyalari xavfsizligini mustahkamlash uchun amalga oshiriladigan qadamlarni belgilaydi, natijalar bo'limi esa ushbu chora-tadbirlarning samaradorligini ta'kidlaydi. Muhokama rivojlanayotgan texnologiyalar va rivojlanayotgan tahdidlarning oqibatlarini qamrab oladi va bu it xavfsizligi tizimini mustahkamlash bo'yicha aniq tavsiyalarga olib keladi.

Kalit So'zlar: Axborot texnologiyalari, xavfsizlik choralari, qoidabuzarliklar, kiberxavfsizlik, xavfni kamaytirish.

Аннотация. В данной статье рассматривается необходимость усиления мер профилактики нарушений в сфере информационных технологий . Анализ литературы исследует различные стратегии, методологии и технологии для снижения рисков и защиты цифровых активов. В разделе "методы" описаны шаги, которые необходимо предпринять для повышения безопасности информационных технологий, а в разделе "Результаты" подчеркивается эффективность этих мер. Обсуждение охватывает новые технологии и последствия новых угроз, что приводит к четким рекомендациям по укреплению системы ИТ-безопасности.

Ключевые слова: информационные технологии, меры безопасности, нарушения, кибербезопасность, снижение рисков.

Annotation. This article considers the need to strengthen measures to prevent violations in the field of information technology . Through the analysis of the literature, various strategies, methodologies and technologies are examined to reduce risks and protect digital assets. The methods division sets out the steps to be taken to strengthen information technology security, while the results division highlights the effectiveness of these measures. The discussion covers emerging technologies and the consequences of emerging threats, and this leads to specific recommendations for strengthening the security system.

ISSN 2181-3187

Keywords: information technology, security measures, violations, Cybersecurity, Risk Reduction.

Zamonaviy raqamli landshaftda axborot texnologiyalari sanoat va jamiyatlarda ajralmas rol o'ynaydi. Biroq, texnologiyaga bu keng tarqalgan ishonch, shuningdek, kiber hujumlardan ma'lumotlarning buzilishiga qadar ko'p qirrali xatarlarga duchor qiladi. Shunday qilib, axborot texnologiyalari sohasidagi buzilishlarning oldini olishga qaratilgan chora-tadbirlarni kuchaytirish zarur. Ushbu maqola axborot texnologiyalari xavfsizligini oshirishga tegishli keng tarqalgan muammolar, metodologiyalar va texnologiyalarni tahlil qilish uchun mavjud adabiyotlarni o'rganadi.

Mavjud adabiyotlarni har tomonlama o'rganish axborot texnologiyalari xavfsizligining zaifliklari va tegishli profilaktika choralari haqida ko'plab tushunchalarni ochib beradi. Tadqiqotlar kiber tahdidlarning, jumladan, zararli dasturlar, fishing hujumlari va to'lov dasturlarining o'sib borayotganini ta'kidlaydi.

Axborot texnologiyalari xavfsizligini oshirish uchun ko'p qirrali yondashuv ajralmas hisoblanadi. Tashkilotlar zarur bilim va ko'nikmalarga ega bo'lgan xodimlarni kuchaytirish uchun kiberxavfsizlik to'g'risida xabardorlik va o'quv dasturlariga ustuvor ahamiyat berishlari kerak. Bundan tashqari, mudofaa chuqur strategiyasini amalga oshirish tarmoqlar, ilovalar va so'nggi nuqtalar bo'ylab xavfsizlik nazorati qatlamlarini joylashtirishni o'z ichiga oladi. Xavfsizlikni muntazam baholash, penetratsion test va zaifliklarni boshqarish potentsial zaif tomonlarni faol ravishda aniqlash va bartaraf etish uchun juda muhimdir.

Axborot texnologiyalari sohasidagi buzilishlarning oldini olish texnologik echimlar, siyosat, qoidalar va ta'limni o'z ichiga olgan ko'p qirrali yondashuvni talab qiladi bu yerda qoidabuzarliklarning oldini olishni yaxshilash bo'yicha ba'zi chora-tadbirlar:

Kuchli kiberxavfsizlik choralari:

- Ruxsatsiz kirish, ma'lumotlar buzilishi va zararli dasturlarning hujumlaridan himoya qilish uchun xavfsizlik devorlari, antivirus dasturlari, kirishni aniqlash tizimlari va shifrlash kabi mustahkam kiberxavfsizlik choralarini amalga oshirish.

- Ma'lum zaifliklarni tuzatish va paydo bo'layotgan tahdidlardan oldinda qolish uchun dasturiy ta'minot va tizimlarni muntazam yangilab turing.

Kirishni boshqarish :

- Faqat vakolatli xodimlarning maxfiy ma'lumotlar va tizimlarga kirishini ta'minlash uchun kirishni qat'iy nazorat qilish siyosatini amalga oshiring.

-Parollardan tashqari qo'shimcha xavfsizlik qatlamini qo'shish uchun ko'p faktorli autentifikatsiyani amalga oshiring.

Xodimlarni o'qitish

ISSN 2181-3187

- Xodimlarga kiberxavfsizlikning eng yaxshi amaliyotlari, jumladan, fishing urinishlarini tan olish, zararli dasturlardan qochish va qurilmalarini himoya qilish bo'yicha keng qamrovli treninglar o'tkazish.

- Kiberxavfsizlik to'g'risida xabardorlik madaniyatini targ'ib qilish, bu erda xodimlar xavfsizlik siyosatiga rioya qilish va shubhali harakatlar haqida xabar berish muhimligini tushunishadi.

Muntazam tekshiruvlar va Muvofiqlikni tekshirish:

- Zaifliklarni aniqlash va me'yoriy talablar va sanoat standartlariga muvofiqligini ta'minlash uchun axborot texnologiyalari tizimlari va tarmoqlarining muntazam tekshiruvlarini o'tkazish.

- Har qanday noodatiy yoki shubhali xatti-harakatlarni aniqlash uchun tarmoq trafigini kuzatish va tahlil qilish jarayonlarini o'rnatish.

Ma'lumotlarni himoya qilish va maxfiylik choralari:

- Maxfiy ma'lumotlarni ruxsatsiz kirish yoki oshkor qilishdan himoya qilish uchun shifrlash, kirishni boshqarish va ma'lumotlarni anonimlashtirish kabi ma'lumotlarni himoya qilish choralarini amalga oshirish.

Hodisalarga javob berish va tabiiy ofatlarni tiklashni rejalashtirish:

- Kiberxavfsizlik hodisalarini aniqlash, ularga javob berish va ularni tiklash tartib-qoidalarini belgilaydigan keng qamrovli voqealarga javob rejasini ishlab chiqish.

- Xavfsizlik buzilgan taqdirda tayyorlikni ta'minlash uchun simulyatsiyalar va mashg'ulotlar orqali hodisalarga javob berish rejasini muntazam ravishda sinab ko'ring.

Sotuvchi va ta'minot zanjiri xavfsizligi:

-Uchinchi tomon sotuvchilari va etkazib beruvchilarining ma'lumotlarni himoya qilish va kiberxavfsizlik bo'yicha tashkilotingiz standartlariga javob berishini ta'minlash uchun xavfsizlik amaliyotini baholang.

- Sotuvchilar uchun xavfsizlik talablari va majburiyatlarini belgilaydigan va har qanday xavfsizlik kamchiliklari uchun ularni javobgarlikka tortadigan shartnoma shartnomalarini tuzing.

Normativ muvofiqlik va qonunchilik bazasi:

- axborot texnologiyalari xavfsizligi bilan bog'liq tegishli qonunlar, qoidalar va sanoat standartlari to'g'risida xabardor bo'ling va qonuniy oqibatlarga yo'l qo'ymaslik uchun muvofiqlikni ta'minlang.

- Kiberxavfsizlikni targ'ib qiluvchi va tashkilotlarni nozik ma'lumotlarni himoya qilish uchun javobgarlikka tortadigan kuchli me'yoriy asoslarni himoya qiling.

Doimiy monitoring va takomillashtirish:

-Real vaqt rejimida yuzaga kelishi mumkin bo'lgan tahdidlarni aniqlash va bartaraf etish uchun it infratuzilmasi va xavfsizlikni nazorat qilishni doimiy monitoring qilish tizimlarini joriy etish.

ISSN 2181-3187

- Rivojlanayotgan kiber tahdidlar va eng yaxshi amaliyotlarga moslashish uchun xavfsizlik siyosati, protseduralari va texnologiyalarini muntazam ravishda ko'rib chiqing va yangilang.

Hamkorlik va axborot almashish:

- Tahdidlarni o'rganish, ilg'or tajribalar va olingan saboqlarni baham ko'rish uchun boshqa tashkilotlar, sanoat sheriklari va davlat idoralari bilan hamkorlikni rivojlantirish.

- Rivojlanayotgan tahdidlar va samarali yumshatish strategiyalaridan xabardor bo'lish uchun axborot almashish tashabbuslari va forumlarida ishtirok etish.

Ushbu chora-tadbirlarni qabul qilish va it xavfsizligi amaliyotini doimiy ravishda takomillashtirish orqali tashkilotlar buzilishlardan himoya qilishni kuchaytirishi va tobora raqamli dunyoda o'z aktivlari, ma'lumotlari va obro'sini himoya qilishi mumkin.

Xulosa va takliflar:

Axborot texnologiyalaridagi buzilishlarning oldini olish bo'yicha chora-tadbirlarni kuchaytirish raqamli aktivlarni himoya qilish va it infratuzilmalarining yaxlitligini ta'minlash uchun zarurdir. Kiberxavfsizlikka nisbatan proaktiv yondashuvni qo'llash orqali tashkilotlar xavflarni samarali ravishda kamaytirishi va potentsial tahdidlarning oldini olishi mumkin. Manfaatdor tomonlar o'rtasidagi hamkorlik, uzluksiz ta'lim va xavfsizlikning innovatsion texnologiyalariga sarmoyalar kiberxavfsizlikning dinamik landshaftida harakat qilishda ajralmas hisoblanadi.

Bundan tashqari, siyosatchilar kiberxavfsizlik tashabbuslarini birinchi o'ringa qo'yishlari va eng yaxshi amaliyotlarga rioya qilishni rag'batlantirish uchun qulay tartibga solish muhitini yaratishlari kerak. Bundan tashqari, shaxslar va tashkilotlar o'rtasida xavfsizlik ongi madaniyatini rivojlantirish kiber tahdidlarga qarshi jamoaviy barqarorlikni mustahkamlashda muhim ahamiyatga ega.

Adabiyotlar.

1. Decree of the President of the Republic of Uzbekistan «On the Strategy of actions for further development of the Republic of Uzbekistan» from 7 February 2017 the year number DP–4947 (in Russian).
2. Resolution of the President of the Republic of Uzbekistan «On measures to radically improve the system of criminal and criminal procedure legislation» from 14 May 2018 the year number PP–3723 (in Russian).
3. Gladkikh V.I. Criminology: textbook (bachelor's and master's degrees). Moscow: Justitia, 2019, 422 p (in Russian).
4. Abdurasulova K. R. Criminology. Textbook. Executive editor: M.Kh.Rustambayev. - T.: «Adolat», 2007. - 216 b (in Uzbek).
5. Criminology. Textbook. Collective of authors. Executive editor: M.Kh.Rustambayev. - T.: TSIL 2008 – 586 p (in Russian).

ISSN 2181-3187

6. Kabulov R., Abdurakhmanov E.S. Crimes in the sphere of information technologies: Textbook. - T.: Academy of the Ministry of internal affairs of the Republic of Uzbekistan, 2009. - 80 p (in Russian).
7. https://www.internetworldstats.com/top20.htm
8. Baxtiyor ogli, R. I. (2023). Methods for searching and using maps using internet resources in geography lessons. *Journal of Universal Science Research*, *1*(11), 545-548.
9. Baxtiyor o'g'li, R. I. (2023). UMUMTA'LIM MAKTABLARIDA GEOGRAFIYANI O'QITISHNING ZAMONAVIY TA'LIM VOSITALARIDAN FOYDALANISH.