2. Khamdamovna, M. U. (2021). The use of Irony in Uzbek Poems as a Speech Decoration. Central Asian Journal of literature, philosophy and culture, 2(11), 17-20. https://doi.org/10.47494/cajlpc.v2i11.242

3. Smith, C. Alphonso. [Ed], Selected Stories from O. Henry. New York, The Odyssey Press, 1922.

4. Utkirovna. N. S. O. Henri hikoyalarining o‘ziga xos yozuv uslubi. // Til, adabiyot, tarjima, adabiy tanqidchilik va zamonaviy yondashuvlar, 2022, 126-128 b.

5. https:en.wikipedia.org/wiki/Stylistics

6. https://www.studiobinder.com/blog/what-are-stylistic-devices-in-literature/

7. https://www.studiobinder.com/blog/what-are-stylistic-devices-in-literature//

BULUTLI PROVAYDERINING JISMONIY VA ATROF-MUHIT XAVFSIZLIK JAVOBGARLIGI

Mamarajabov Odil Elmurzayevich

Nizomiy nomidagi TDPU

Axborot texnologiyalari kafedrasi v/b dosenti

Axmatov Eldor Umar o‘g‘li

Nizomiy nomidagi TDPU

Axborot tizimlari va texnologiyalari 3-bosqich talabasi

Bulut provayderining javobgarligi jismoniy xavfsizlik va atrof-muhit xavfsizligidan boshlanadi. Xavfsizlikning ushbu darajasi yuqori darajadagi darajadir, chunki u bulutni birlashgan axborot tizimi sifatida boshqarilishi bilan bog`liq. Ma’lumot markazlarining jismoniy serverlarini boshqaradigan bulutli xizmat ko`rsatuvchi provayder, shuning uchun mijoz odatdagi ma’lumotlar markazida bo`lgani kabi quyidagi asosiy fikrlarni ko`rib chiqishi kerak: xodimlarning serverlarga va tarmoq infratuzilmasiga jismoniy kirishi, yong`in signalizatsiyasi va

yong`in o`chirish uskunalari, serverlar va boshqa jihozlar ustidan iqlim va haroratni nazorat qilish, ishdan chiqarilgan saqlash moslamalarini yo‘q qilish.

Jismoniy xavfsizligidan farqli o`laroq, tarmoq xavfsizligi, birinchi navbatda, tajovuzdan himoya va xavfsizlik devorlarini o`z ichiga olgan kuchli tahdid modelini yaratish bilan bog`liq. Xavfsizlik devoridan foydalanish ma’lumotlar markazining ichki tarmoqlarini turli darajadagi ishonchga ega subnetlarga ajratish uchun filtr ishini nazarda tutadi. Bu Internetdan foydalanish mumkin bo`lgan alohida serverlar yoki ichki tarmoqlardan serverlar bo`lishi mumkin.

Bulutli hisoblash quvvatini boshqarish uchun Internetga kirish bulutli hisoblashning asosiy xususiyatlaridan biridir. Ko`pgina an'anaviy ma’lumotlar markazlarida muhandislarning serverlarga kirishi jismoniy darajada nazorat qilinadi, bulutli muhitda ular Internet orqali ishlaydi. Kirish nazoratini cheklash va tizim darajasidagi o`zgarishlarning shaffofligini ta’minlash asosiy himoya mezonlaridan biridir.

Xuddi shunday, bulutni tarqatish modelini tanlash ham xavfsizlikning umumiy darajasiga ta’sir qiladi: xususiy bulut, yagona tashkilotdan eksklyuziv foydalanish uchun tayyorlangan infratuzilma; ommaviy bulut, foydalanuvchilarning keng doirasi tomonidan bepul foydalanish uchun mo`ljallangan infratuzilma; umumiy bulut, umumiy maqsadlarga ega bo`lgan tashkilotlarning iste'molchilarning ma’lum bir jamoasi tomonidan foydalanishga mo`ljallangan infratuzilmaning bir turi; va gibrid bulut, ikki yoki undan ortiq turli xil bulut infratuzilmalarining kombinatsiyasi.

Xususiy bulutlar eng xavfsiz hisoblanadi, chunki ular shaxsiy shifrlash va himoya vositalarning yaratilish bosqichida amalga oshirishga imkon beradi, shuningdek, ma’lumotlar kompaniyaning mavjud infratuzilmasida qoladi. Ammo, agar ma’lumotlar bulutda to`g`ri himoyalanmagan bo`lsa, bulut xususiy yoki jamoat bo`lishidan qat'i nazar, ular yo‘qolishi yoki buzilishi mumkin. Xususan, tizim ichkarisida ishonchli kirish huquqiga ega bo`lgan vijdonsiz shaxslar himoyalanmagan ma’lumotlarni ko`rishlari, buzishlari va o`g`irlashlari mumkin. Ichki tahdidlar tahdidlarning ayrim yangi turlari emas, ammo korporativ ma’lumotlar markazlari virtualga o`tganda, kirishni boshqarishning an'anaviy mexanizmlari samarasiz bo`lib,

virtual maydonga moslashtirilmaydi. Masalan, ma’lumotlar bazasi nusxasini yangi jismoniy serverga o`rnatmoqchi bo`lganingizda, o`zgarishlarni boshqarish protseduralari qo`llaniladi. O`zgarishlarni boshqarish - bu kelajakdagi o`zgarishlarni bashorat qilish va rejalashtirish, batafsil o`rganish uchun barcha mumkin bo`lgan o`zgarishlarni ro`yxatdan o`tkazish, oqibatlarini baholash, tasdiqlash yoki rad etish, shuningdek, loyihadagi o`zgarishlarni amalga oshiruvchi ijrochilarning monitoringi va muvofiqlashtirilishini tashkil etish jarayoni. Virtual xususiy bulutda mavjud bo`lgan virtual serverni klonlash orqali yangi ma’lumotlar bazasi misoli yaratilishi mumkin. Agar himoyalangan serverdan ma’lumotlar himoyalanmaganga o`tkazilsa, ushbu ma’lumotlarni ushbu shaxsiy bulutda kirish huquqi past foydalanuvchilar ko`rishlari mumkin.

Xavfsizlik tizimlari tomonidan boshqarilmaydigan ko`r zonaning mavjudligi - bulutdagi virtual serverlar o`rtasidagi trafik. An'anaviy kuzatuv vositalari ushbu trafikni ushlab turish va tahlil qilishga qodir bo`lgan tarmoq qurilmalari va sensorlar portlaridagi trafikni aks ettirish orqali ishlaydi. Shu bilan birga, VMlar o`rtasida ma’lumotlar uzatish kanallari gipervizorda yaratiladi. Zararli trafik va ma’lumotlar VM-lar orasida haqiqiy tarmoqqa chiqmasdan xarakatlanishi mumkin, demak, hujum an'anaviy vositalar tomonidan sezilmaydi.

O`chirib qo`yilgan VM-larda saqlanadigan ma’lumotlar, agar u joylashgan asosiy operatsion tizimida kirish nazorati to`g`ri sozlanmagan bo`lsa yoki muhim zaifliklarni tuzatuvchi yangilanishlar o`rnatilmagan bo`lsa, himoyasiz bo`ladi.

Jamoat bulutidan foydalangan holda, tashkilotlar bulut (IaaS), platforma (PaaS) va dasturiy ta’minot (SaaS) tarkibidagi provayderning infratuzilmasidan foydalanishlari mumkin. Ma’lumotlar tijorat ma’lumotlar markazlarining ijaraga olingan infratuzilmasidan foydalangan holda bulutli provayder muhitida saqlanadi. Ko`pgina hollarda, jamoat bulutlarini tejash umumiy jismoniy resurslardan yanada samarali foydalanish natijasida yuzaga keladi. Bu shuni anglatadiki, mijozlarga bir xil jismoniy serverda joylashtirilgan turli xil VM-fayllarni taqdim etish va mijozning bir xil xizmat yoki dasturga boshqa hisoblar ostida kirishini tashkil qilish mumkin. Masalan, salesforce. comning mashhur bulutga asoslangan CRM ilovasi ruxsatsiz

kirishni oldini olish uchun noyob kirish orqali turli xil mijozlarga bir xil xizmatni taqdim etishning bir misoli bo`la oladi, garchi turli xil foydalanuvchilar ma’lumotlari bir xil omborda aralashgan bo`lsa ham. Har qanday holatda, virtualizatsiyadan foydalanganda, ushbu texnologiya bilan bog`liq bo`lgan barcha axborot xavfsizligi muammolarini hisobga olish kerak.

Albatta, ommaviy bulut doirasida, shuningdek, mijozga butunlay alohida, bag`ishlangan kompyuter resursini taqdim etish mumkin, bu, xususan, monitoring va auditni yaxshiro? o`tkazish imkonini beradi. Biroq, ushbu qo`shimcha xavfsizlik qulayligi ko`pincha bulutli resurslardan foydalanish narxining sezilarli darajada oshishi bilan birga keladi, bu odatda o`zlarining ma’lumot markazlariga nisbatan bunday manbalarning afzalliklarini kamaytirishi mumkin.

Jamoat bulutida axborot xavfsizligiga klassik tahdidlar ayniqsa dolzarb bo`lib qolmoqda. Masalan, katta bulutli resurs ma’muri ko`plab mijozlarning ma’lumotlariga kirish huquqiga ega. U ushbu ma’lumotlarga ruxsatsiz xattixarakatlarni osongina amalga oshirishi mumkin, ammo bunday hodisalar, umuman, hech qachon aniqlanmasligi mumkin. Masofaviy xakerlik hujumlari kabi tashqi xavfsizlik tahdidlari ham mavjud. Ommaviy bulutlar juda ko`p miqdordagi korporativ ma’lumotlarga ega, bu ularni tajovuzkorlar uchun jozibali qiladi. 100 ta kompaniyaning ma’lumotlarini o`z ichiga olgan resursning veb-dasturida zaifliklarni topish bitta kompaniyaning veb-dasturini buzishdan ko`ra ancha qiziqroq. Xuddi shunday, ko`plab yirik kompaniyalarning tarmoqdagi zaxira omboriga hujum qilish, faqat bitta tashkilotga tegishli bo`lgan saqlashga zarar etkazishdan ko`ra ko`proq ma’lumot olish mumkin.

Foydalanilgan adabiyotlar

1. Абдурахманова, Ш. А., & Хасанов, А. А. (2019). Применение wiki-технологий в образовании. *профессионально-педагогическая культура учителя и преподавателя: содержание, модели и технологии образовательной деятельности*, 95.

2. Abduxakimovna, A. S., & Mikhailovich, Y. V. (2023). Application of digital learning technologies in vocational education. *образование наука и инновационные идеи в мире*, *22*(1), 143-145.

3. Mamarajabov Odil Elmurzaevich, Akhmatov Eldor Umar ugli, Creating an electronic textbook on computer science in the autoplay program , E Conference World: No. 2 (2023): Switzerland

4. Elmurzayevich, Mamarajabov O. "Cloud Technology to Ensure the Protection of Fundamental Methods and Use of Information." International Journal on Integrated Education, vol. 3, no. 10, 2020, pp. 313-315, doi:10.31149/ijie.v3i10.780.

5. Muratov, E. I. (2020). Improving the quality of the educational system of higher educational institutions by means of the involvement of students in the educational process with the use of analytical possibilities of neural network technologies. Theoretical & Applied Science, (9), 21-23.

6. Bagbekova Laylo Kadirbergenovna, Khusanbayev Elmurod Ubaydulla ugli Methodology for organizing the process of distance education and its teaching. (2023). E Conference World, 2, 160-164. https://econferenceworld.org/index.php/ecw/article/view/42

7. Bagbekova Laylo Kadirbergenovna Distance education system as a modern method of training. (2023). E Conference World, 2, 97-102. https://econferenceworld.org/index.php/ecw/article/view/32

8. Qizi, U. S. B. (2022). The role of video production in modern pedagogical technologies.

9. Хасанов, А. А., & Ўроқова, Ш. Б. Қ. (2021). Цифровизация образования на современном этапе развития информатизированного общества. Scientific progress, 2(1), 300-308.

10. Bakiyeva, Z. (2022). Teaching the steps of creating animation to students in higher education institutions. Академические исследования в современной науке, 1(17), 226-227.