BULUTLI HISOBLASH PROVAYDERLARI RISKLARNI BOSHQARISH TIZIMI TAHLILI

Nasrullayev Nurbek Baxtiyorovich
(Muhammad al-Xorazmiy nomidagi TATU Nurafshon filiali, PhD)

Shirinov Laziz Toxirovich
Muhammad al Xorazmiy nomidagi TATU, doktorant
shirinovlaziz05@gmail.com

ANNOTATSIYA

Ushbu maqolada bulutli hisoblash provayderlari uchun ularning turlari va modellaridan qat'i nazar, NIST risklarni boshqarish jarayoni va risklarni boshqarish tizimi taklif etiladi. Bulutli hisoblash provayderlari asosan mahsulot va xizmatlarni taqdim etish va o'z foydalariga xizmat qilishi bayon etilgan.

Kalit so'zlar: *bulut, risk, Risk Management Framework, RMF, tahdid, cloud computing.*

CLOUD COMPUTING PROVIDERS RISK MANAGEMENT SYSTEM ANALYSIS

ABSTRACT

This article offers NIST Risk Management Process and risk management system for cloud computing providers regardless of their types and models. It is stated that cloud computing providers mainly provide products and services and serve their benefits.

Keywords: *cloud, risk, Risk Management Framework, RMF, threat, cloud computing.*

KIRISH

Hisoblash resurslari va xizmatlarini taqdim etishning turli usullari orasida bulutli hisoblash provayderi Internet infratuzilmasi bo'yicha eng yaxshi o'z-o'ziga xizmatlardan biridir. Bulutli hisoblash provayderining asosiy vazifasi shundan iboratki, har bir foydalanuvchi o'z joylashuvi va qurilmalarining asosiy operatsion tizimidan qat'i nazar, mavjud ilovalardan foydalanishi va xizmatlarni osongina olishi mumkin. Ularning biznes maqsadi yuqori risksiz va ishonchli ilovalar va xizmatlarni

taqdim etishdir. Bundan tashqari, ular mijozning ishonchi va sodiqligini qozonishni maqsad qilishadi.

Bulutli hisoblash provayderlari riskli risksizlik xatarlari va muammolariga duch kelishdi. Ushbu muammolar provayder xizmatlarining maxfiyligi, maxfiyligi, ishonchliligi va yaxlitligiga salbiy ta'sir ko'rsatishi mumkin. Shuning uchun, risksizlik risklari va hisoblash aspektidagi muammolarni hal qilish uchun Risk Management Framework (RMF) deb nomlangan maxsus risklarni boshqarish jarayoni tavsiya etiladi. RMF ning asosiy g'oyasi oddiygina "dastur risksizligi riskini vaqt o'tishi bilan o'zgarganligini aniqlash, tartiblash, kuzatish va tushunish" hisobalnadi. Ushbu keng doira moslashuvchanlikni ta'minlashda ishlatilishi mumkin, chunki bu kichik va yirik korxonalarga mos kelishi mumkin. Shuningdek, "RMF risksizlik xatarlariga xos emas; u dasturiy ta'minot bo'lmagan holatlarda qo'llanilishi mumkin". Bulutli hisoblashda RMF dan foydalanadigan provayderlarning asosiy maqsadi risklarni doimiy ravishda kuzatib borish va boshqarishdir.

Har qanday tashkilotda risklarni boshqarishni qo'llashning aniq maqsadi tashkilotlarga salbiy ta'sirlarni minimallashtirish bo'yicha qaror qabul qilishdir.

RISKLARNI IDENTIFIKATSIYA QILISH

Riskni identifikatsiya qilish - bu axborot tizimlariga va ular bilan bog'liq jarayonlarga zarar yetkazishi mumkin bo'lgan hodisalarni aniqlash jarayonidir. Xalqaro Standartlashtirish Tashkiloti (ISO) va Xalqaro Elektrotexnika Komissiya (IEC) ma'lumotlariga ko'ra, risklarni aniqlash uchun turli yondashuvlardan foydalanishi mumkin [1].

Asosiy yondashuvda tashkilot o'zining mavjud risksizlik choralari bilan solishtirganda kamchiliklarni biladi. Ratarlarni batafsil tahlil qilish yondashuvi tashkilotdagi axborot tizimlarini chuqur tahlil qilishni o'z ichiga oladi; nihoyat, yuqoridagi kombinatsiyalangan yondashuvlar gibrid tarzda qo'llaniladi. Masalan, tashkilotdagi odamlar muhim axborot tizimlarini norasmiy tarzda aniqlashlari mumkin. Keyinchalik, tanqidiy tizimlarga potentsial hodisalarni aniqlash uchun batafsil risk tahlili yondashuvi qo'llaniladi. Boshqa tizimlar uchun asosiy yondashuv qo'llaniladi. Risklarni batafsil tahlil qilish yondashuvi muhim tizimlar uchun potentsial hodisalarni aniqlash uchun ishlatiladi. Boshqa tizimlar uchun asosiy yondashuv qo'llaniladi. Risklarni batafsil tahlil qilish yondashuvi muhim tizimlar uchun potentsial hodisalarni aniqlash uchun ishlatiladi. Boshqa tizimlar uchun asosiy yondashuv qo'llaniladi.

Risklarni baholash. Risklarni baholash - bu aniqlangan potentsial hodisalarning miqdoriy yoki sifat jihatidan ta'sirini bashorat qilish jarayonidir. Risklarga pul qiymatlarini belgilash o'rniga, OCTACE, ISRAM, CRAMM va boshqalar kabi sifat sxemasi risklarni nisbiy darajalar bo'yicha baholash imkonini beradi. Umuman olganda, sifat sxemasi miqdoriy sxemaga qaraganda risksizlik yoki kompyuter

bo‘yicha mutaxassis bo‘lmagan odamlar tomonidan bajarilishi va tushunilishi osonroq [2].

Riskni davolash. Potentsial hodisa aniqlangan va baholangandan so‘ng, tashkilot riskni qanday davolash kerakligini hal qilishi kerak. Mumkin variantlarga quyidagilar kiradi:

(1) Hech narsa qilmaslik va riskni qabul qilish.
(2) Tegishli harakatlar yoki biznes jarayonlarini o‘zgartirish yoki tugatish orqali yuzaga kelishi mumkin bo‘lgan hodisalarning oldini olish.
(3) Sug‘urtalash yoki risklarni boshqa tomonlarga o‘tkazish.
(4) Risklarni maqbul darajaga kamaytirish uchun tegishli risksizlik choralarini qo‘llash.

Bir nechta himoya turlari mavjud. Agar bir xil potentsial hodisaga bir nechta risksizlik choralarini qo‘llash mumkin bo‘lsa, tashkilot o‘zining risksizlik investitsiyasini optimallashtirish uchun foyda-xarajat tahlili yoki boshqa yondashuvdan foydalanishi mumkin.

Risklarni monitoring qilish va qayta baholash. Risklarni baholash va davolashning to‘g‘riligi va samaradorligini ta’minlash uchun qoldiq risklar va aniqlangan qabul qilinadigan risklar muntazam ravishda monitoring qilinishi va ko‘rib chiqilishi kerak. Bundan tashqari, tashkilot tashkilotdagi katta o‘zgarishlarni aks ettirish uchun o‘z risklarini qayta baholashi kerak bo‘lishi mumkin.

Tanimoto, Xiramoto, Iwashita, Sato va Kanai (2011) [4] risklarni taqsimlash strukturasi (RBS) usuli va risk matritsasi usuli asosida bulutli hisoblash risksizligi muammolarini batafsil tahlil qildi. Ular foydalanuvchi nuqtai nazaridan kelib chiqadigan risklarni taqdim etdi. Xie, Peng, Zhao, Chen, Wang and Huo (2012) bulutli hisoblash uchun risklarni boshqarish tizimini taklif qildi, u besh komponentdan iborat [5]:

1. foydalanuvchi talabini o‘z-o‘zini baholash;
2. bulutli xizmat ko‘rsatuvchi provayderlarning ish stolini baholash;
3. risklarni baholash;
4. uchinchi tomon agentliklari tekshiruvi;
5. doimiy monitoring.

Risklarni boshqarish tizimining doirasi Xie va boshqalar bilan solishtirganda farq qiladi. Ularning doirasida foydalanuvchilar, provayderlar va uchinchi tomon ishtirok etadi. Shu bilan birga, biz ushbu doirada biznes burchagini ta’kidlaymiz; biznes va texnik muammolarning o‘zaro bog‘lanishi bizning risklarni boshqarish rejamizning asosiy omilidir. Shuningdek, bulutli hisoblashni qabul qiluvchilar va foydalanuvchilarni ko‘paytirish ushbu doira maqsadlaridan biridir. Bulutli hisoblashning tarqalishi uchun foydalanuvchilar xizmat ko‘rsatuvchi provayderlar o‘z

ma’lumotlarini himoya qilish usullariga yuqori darajadagi ishonchga ega bo‘lishlari kerak. Taklif etilayotgan RMF olti bosqichdan iborat bo‘lib, ular keyingi bo‘limda batafsil muhokama qilinadi. Biroq, boshqa doiralar besh yoki undan kam bosqichdan iborat. Bulutli hisoblash muammolari bilan bog‘liq ta’sirlarni minimallashtirish uchun, agar tashkilotlar tizimlar va ma’lumotlarni himoya qilish va himoya qilishda bulutli hisoblashning ko‘plab afzalliklaridan foydalanmoqchi bo‘lsa, riskni kamaytirish zarur.

RMF BOSQICHLARI

RMF oltita asosiy faoliyat bosqichidan iborat:

(1) biznes kontekstini tushunish;
(2) biznesning texnik riskini aniqlash;
(3) riskni sintez qilish va ustuvorlik qilish;
(4) riskni kamaytirish strategiyasini aniqlash;
(5) talab qilinadigan ishlarni bajarish yechimlar va ularning hal qilinganligini tasdiqlash;
(6) tizimni umumiy baholash va monitoring qilish;

Har bir bosqich quyida batafsil muhokama qilinadi.

Risklarni sintez qilish. Har qanday tizimda har doim katta miqdordagi risk mavjud bo‘ladi. Ushbu bosqichda ustuvorliklarni belgilash jarayonida faoliyatning eng muhim maqsadlari va qaysi maqsadlar darhol tahdid qilinishini hisobga olish kerak.

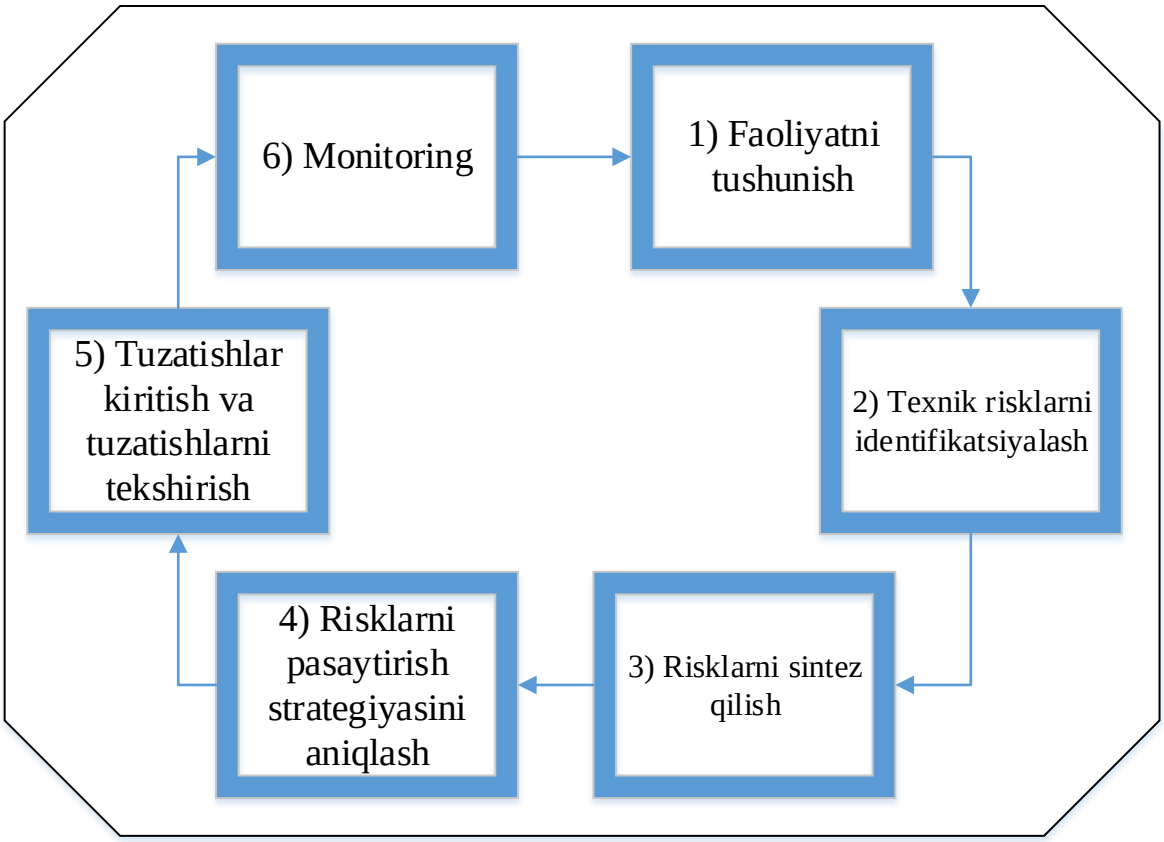
Xatarni kamaytirish strategiyasini belgilash. Ushbu bosqichda xatarlarni tejamkorlik bilan kamaytirish uchun izchil strategiya yaratilishi kerak. Taklif etilgan yumshatish bo‘yicha har qanday chora-tadbirlar xarajatlarni, amalga oshirish vaqtini, muvaffaqiyat ehtimolini, to‘liqligini va risklarning butun majmuasiga ta’sirini hisobga olishi kerak.

Kerakli yechimlarni amalga oshirish va ularni hal qilinganligini tasdiqlash. Ushbu bosqich tekshirish usullarini amalga oshirishni o‘z ichiga oladi, bu holatni yaxshilash orqali risklar to‘g‘ri yumshatilganiga va strategiya ishlayotganiga ishonch hosil qiladi. Bundan tashqari, yumshatish strategiyasi samarali ekanligiga ishonch hosil qilish uchun sinovdan o‘tkazilishi kerak.

Umumiy baholash va monitoring bosqichi. Kerakli yechimni amalga oshirgandan so‘ng, qo‘llaniladigan yechimning natijasini doimiy ravishda baholash uchun ekspertlar guruhlari yig‘iladi. Kuzatishlar asosida umumiy riskni baholash rejaga mos keladimi yoki yo‘qmi, har bir vaziyatda keyin nima qilish kerakligi haqida qaror qabul qiladi. Agar riskni baholash rejaga javob bersa, ular tahdid turini va samarali yechimlarni hujjatlashtirishi mumkin. Keyin ular yechimning zaif tomonlari va ularni tuzatish yo‘llari haqida o‘ylashlari mumkin. Bundan tashqari, agar mavjud yechim shunga o‘xshash hujum ko‘rinishida muvaffaqiyatsiz bo‘lsa, tayyorlikni oshirish uchun muqobil yechimlar ham ishlab chiqilishi mumkin. Mutaxassislar,

shuningdek, biznes sheriklarining maqsadlariga erishish, shuningdek, mijozlarning ishonchini ta’minlash samaradorligini ko‘rish uchun yechim samaradorligini baholashlari mumkin. Agar yechim muvaffaqiyatsiz bo‘lsa, Mutaxassislar yechim nima uchun muvaffaqiyatsizlikka uchraganini baholab, uni tuzatish yo‘llarini o‘ylab topishlari mumkin. Ular zarar darajasini baholashlari va bunday hujumlardan keyin har qanday oqibatlarga qarshi kurashishning samarali usullarini topishlari mumkin.

Uzluksiz risklarni boshqarish jarayoni bulutli hisoblashda zaruratdir. Shuningdek, doimiy risklarni aniqlash, amalga oshirish va baholash orqali doimiy monitoring jarayoni talab qilinadi. Xatarlarni boshqarish rejasi yaxshi tashkil etilgan bo‘lishi kerak, bu turli bo‘limlar o‘rtasida va o‘rtasida hamkorlikni talab qiladi. Rejalashtirish, tashkil etish, hamkorlik va muloqot qilish uchun yetarli vaqt berilishi kerak.



1-rasm. RMF oltita asosiy faoliyat bosqichidan iborat

Yuqoridagi 1-rasmda o‘rtada kutilgan narsa haqiqatda ishlayotganiga ishonch hosil qilish uchun butun jarayon davomida monitoring zarurligini ko‘rsatadi. Bu risklarni boshqarish hujjatlarida belgilangan izchil vaqt oralig‘ida amalga oshirilishi kerak. Ba’zan joylarga muddat belgilash kerak bo‘ladi va boshqa paytlarda ma’lum bir jarayonni o‘zgartirish oqilona bo‘ladi. Agar jarayon o‘zgartirilgan bo‘lsa, u risklarni

boshqarish hujjatlariga qo‘shiladi. Ba’zi tashkilotlar monitoringni autsorsing orqali hal qilishni afzal ko‘radi, boshqalari esa monitoringni o‘zida olib boradi. Bulutli xizmatlarni kuzatishda hujjatlarda harakatchanlikni yaxshiroq shakllantirish uchun bir nechta turli kompaniyalar o‘rtasida jamoa tuzish mantiqan to‘g‘ri bo‘lishi mumkin.

Shuningdek, 1-rasmning o‘rtasida u aloqa va konsalting haqida keltirilgan. Bu shuni anglatadiki, barcha manfaatdor tomonlarni risklarni boshqarish hujjatlarida nima deyilganligi haqida xabardor qilish kerak va agar u o‘zgartirilsa, barcha manfaatdor tomonlar bilan bog‘lanish kerak bo‘ladi. Shu sababli monitoringni autsorsing qilish hozirda bulutli hisoblash texnologiyasida keng qo‘llaniladi. Kichik biznesda o‘z tizimlarini kuzatishda manfaatdor tomonlar bilan doimiy suhbatlashish uchun resurslar yetishmaydi.

Birinchi bosqichda, ya’ni riskni baholash va identifikatsiyalashga tayyorgarlik, turli xil ma’lumotlar, shu jumladan miqdoriy va sifat ma’lumotlari to‘planadi. Tizim tahlilchilari turli odamlar (masalan, menejer, IT boshqaruvi, mijozlar, ishlab chiquvchilar, xodimlar) intervyu va so‘rov o‘tkazish uchun bir nechta savollarni ishlab chiqishi kerak. Bu savollar biznes maqsadlari va missiyasi, oyiga o‘rtacha yangi va tark etuvchi mijozlar, biznes profili va funktsiyalari, o‘rtacha daromad, reklama va marketing, resurs yetkazib beruvchilar, mijozlar da’volari, joriy texnik nuqsonlar va himoya usullari, tizimga murojaat qilishi mumkin. Bundan tashqari, ularga umumiy tizimni o‘rganish va uni kichik qismlarga ajratish uchun tadqiqot loyihasini ishlab chiqish tavsiya etiladi. Shuningdek, diqqat qilish uchun tegishli muhim sohalarni tanlash zarur; ayniqsa hududga zudlik bilan e’tibor berish kerak.

1-jadval maqsadlarni federal qoidalarda talab qilinadigan standartlarga samarali javob beradigan tarzda tartiblash bo‘yicha ko‘rsatmalar beradi (NISTning biznes maqsadlarini tartiblash bo‘yicha taxminiy ko‘rsatmalaridan foydalanish mumkin). Ushbu reyting biznes maqsadlarini loyihaga, xodimlarga va umuman kompaniyaga ta’siri darajasiga qarab, Oliy (H), O‘rta (M) va Past (L) daraja ostida joylashtiradi. Maqsad, agar u loyihaning mavjudligi va davom etishi uchun hal qiluvchi ahamiyatga ega bo‘lsa, yuqori o‘rinni egallaydi. Bunday maqsadlarning muvaffaqiyatsizligi butun loyihani to‘xtatib qo‘yishi va kompaniyaga bevosita ta’sir qilishi mumkin. O‘rta darajali maqsadlar loyihaning mavjudligi uchun juda muhimdir va ularning muvaffaqiyatsizligi ko‘plab xodimlarga salbiy ta’sir ko‘rsatishi va yuqori darajali maqsadlarni ham berishi mumkin [3].

1-jadval. NIST tomonidan biznes maqsadlari reytingi bo‘yicha ko‘rsatmalar

Daraja	Ta’rif
Yuqori	Ushbu maqsadlar loyihaning (va ehtimol kompaniyaning) mavjudligi uchun juda muhimdir. Agar ushbu maqsadlarga erishilmasa, loyiha o‘z faoliyatini to‘xtatib qo‘yishi va kompaniyaga bevosita ta’sir qilish riski mavjud.
O‘rta	Ushbu maqsadlar loyihaning (va ehtimol kompaniyaning) mavjudligi uchun juda muhimdir. Agar ushbu maqsadlar bajarilmasa, ko‘plab xodimlar ta’sir qilishi mumkin. O‘rta darajadagi biznes maqsadiga erisha olmaslik yuqori darajadagi maqsadlarga salbiy ta’sir ko‘rsatishi mumkin.
Past	Ushbu maqsadlar kompaniya daromadining faqat kichik bir qismiga ta’sir qiladi. Agar ushbu maqsadlar bajarilmasa, oz sonli xodimlar ta’sir qilishi mumkin.

Risklarni boshqarish rejasining yo‘nalishlari, qo‘mitalari, maqsadlari, talablari, muddati va hajmini yaratish boshida amalga oshirilishi kerak. Buni amalga oshirishdan maqsad qo‘mitalardagi har bir kishi o‘z mas’uliyati, roli va vaqtini bilishini ta’minlashdan iborat. Bundan tashqari, bu harakatlarni yanada samarali va to‘g‘ridan-to‘g‘ri sarflashga yordam beradi.

Ikkinchi bosqich riskni tahlil qilish va baholashni o‘z ichiga oladi. Biznes va texnik risklarni aniqlashda tahdidlarning uchta asosiy manbasini hisobga olish kerak:

tabiiy (masalan, suv toshqini, zilzilalar, tornadolar),

inson omili (shu jumladan, qasddan bo‘lmagan harakatlar va tarmoq hujumlari kabi qasddan qilingan harakatlar)

muhit tahdidlari (masalan, uzoq muddatli risklar).

Ushbu toifalar orasida eng ko‘zga ko‘ringanlari g‘arazli niyatdagi hujumchilaridir. Hujumni amalga oshirish uchun motivatsiya va manbalar odamlarni potentsial riskli tahdid manbalariga aylantiradi. 2-jadvalda bugungi kundagi ko‘plab inson tomonidan tahdidlar, ularning mumkin bo‘lgan motivatsiyalar va hujumni amalga oshirishi mumkin bo‘lgan usullar yoki tahdid harakatlari ko‘rsatilgan.

Shuningdek, ushbu manbalarni ikkita keng toifaga bo‘lish mumkin, ya’ni qarama-qarshi va qarama-qarshiliksiz hodisalar. Qarama-qarshi hodisalar asosan xakerlar va kiberjinoyatchilar tashkilotlari kabi insoniy dushmanlar tomonidan boshlangan voqealardir. Shu bilan birga, noaniq hodisalar zilzila, suv toshqini, tizimdagi nosozlik kabi ekologik muammolar tufayli yoki beixtiyor operatorlar tomonidan sodir bo‘ladi [6].

2-jadval. Inson tomonidan amalga oshiriladigan tahdidlar: tahdid manbai, motivatsiya va tahdid harakatlari

Tahdid manbai	Motivatsiya	Tahdid harakatlari
Buzg‘unchi (Hacker, kraker)	O‘zini ko‘rsatib qo‘yish, moliyaviy rag‘bat	• Xakerlik • Ijtimoiy muhandislik • Tizimga kirish, buzish • Tizimga ruxsatsiz kirish
Kompyuter jinoyatchisi	Ma’lumotni yo‘q qilish Noqonuniy ma’lumotlarni oshkor qilish Pul daromadlari Ma’lumotlarni ruxsatsiz o‘zgartirish	• Kompyuter jinoyati (masalan, kiber ta’qib) • Firibgarlik harakati (masalan, o‘zini namoyon qilish, tinglash) • Axborot poraxo‘rligi • Soxtakorlik • Tizimga ruxsatsiz kirish
Terrorchi	Qasd qilish, o‘z manfaatida foydalanish	• Bomba/Terrorizm • Axborot urushi • Tizimga hujum (masalan, tarqatilgan xizmatni rad etish) • Tizimga kirib borish • Tizimni buzish
Sanoat josusligi (kompaniyalar, xorijiy hukumatlar, boshqa davlat manfaatlari)	Raqobat ustunligi Iqtisodiy josuslik	• Iqtisodiy ekspluatatsiya • Axborot o‘g‘irlanishi • Shaxsiy maxfiylikka tajovuz • Ijtimoiy muhandislik • Tizimga kirish • Tizimga ruxsatsiz kirish (maxfiy, xususiy va/yoki texnologiya bilan bog‘liq ma’lumotlarga kirish)
Insayderlar (yomon o‘qitilgan, norozi, yomon niyatli, beparvo, insofsiz yoki ishdan bo‘shatilgan xodimlar)	CuriosityEgoIntelligence Pul daromadi Qasos Qasddan bo‘lmagan xatolar va kamchiliklar (masalan, ma’lumotlarni kiritish xatosi, dasturlash xatosi)	• Xodimga hujum qilish • Shantaj • Shaxsiy ma’lumotlarni ko‘rib chiqish • Vokolatni suiiste’mol qilish • Firibgarlik va o‘g‘irlik • Axborot poraxo‘rlik • Soxta, buzilgan ma’lumotlarni qo‘lga kiritish • Zararkunanda dastur • Shaxsiy ma’lumotlarni sotish • Tizimdagi xatolar • Tizimga kirish • Tizimga sabotaj • Tizimga ruxsatsiz kirish

XULOSA

Xulosa qilib aytganda, risklar va zaifliklarni olib tashlagandan so‘ng, risk ko‘rsatkichlari, risklarning ta’siri va aniqlangan risklarning yuzaga kelish ehtimoli yaratilishi kerak Bundan tashqari, ushbu bosqich texnik risklarni aniqlash va tavsiflashni hamda ularni biznes maqsadlari bilan bog‘lashni o‘z ichiga oladi. Muammoning yuzaga kelish ehtimoli qanchalik yuqori bo‘lsa, salbiy ta’sirni hisobga olish biznes tomonidan riskni baholashning asosiy ko‘rsatkichi sifatida ishlatilishi mumkin. Ta’sir darajasi va yuzaga kelish ehtimoli tahlilchiga biznes riskining turli biznes maqsadlariga ta’sirini baholash imkonini beradi. Bundan tashqari, ushbu bosqich texnik risklarni aniqlash va tavsiflashni va ularni biznes maqsadlari bilan bog‘lashni o‘z ichiga oladi.

ADABIYOTLAR RO‘YXATI

1. Brender, Nathalie, & Markov, Iliya. (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. International Journal of Information Management, 33(5), 726-733. doi: 10.1016/j.ijinfomgt.2013.05.004

2. Chonka, Ashley, Xiang, Yang, Zhou, Wanlei, & Bonti, Alessio. (2011). Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications, 34(4), 1097-1107. doi: 10.1016/j.jnca.2010.06.004

3. Liu, Wentao. (2012). Research on cloud computing security problem and strategy. Paper presented at the Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on.

4. Salah, Khaled, Calero, Jose M. Alcaraz, Zeadally, Sherali, Al-Mulla, Sameera, & Alzaabi, Mohammed. (2013). Using cloud computing to implement a security overlay network. IEEE Security & Privacy, 44-53.

5. Xia, Li. (2012, 2012/10//). Issue about Security of E-business Under the Pattern of Cloud Computing.

6. Xiao, Zhifeng, & Xiao, Yang. (2013). Security and privacy in cloud computing. Communications Surveys & Tutorials, IEEE, 15(2), 843-859.