MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI

FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

"AL-FARG'ONIY AVLODLARI"

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI

1-SON 1(5)
2024-YIL

TATU, FARG'ONA
O'ZBEKISTON

ISSN 2181-4252

O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI FARG‘ONA FILIALI

Muassis: Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali.
Chop etish tili: O‘zbek, ingliz, rus.
Jurnal texnika fanlariga ixtisoslashgan bo‘lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo‘nalishida maqolalar chop etib boradi.

Учредитель: Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.
Язык издания: узбекский, английский, русский.
Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

Founder: Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.
Language of publication: Uzbek, English, Russian.
The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

2024 yil, Tom 1, №1
Vol.1, Iss.1, 2024 y

ELEKTRON ILMIY JURNALI **ELECTRONIC SCIENTIFIC JOURNAL**

«Al-Farg‘oniy avlodlari» («The descendants of al-Fargani», «Potomki al-Fergani») O‘zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro‘yxatdan o‘tgan.

Jurnal OAK Rayosatining 2023-yil 30 sentabrdagi 343-sonli qarori bilan Texnika fanlari yo‘nalishida milliy nashrlar ro‘yxatiga kiritilgan.

Tahririyat manzili:
151100, Farg‘ona sh.,
Aeroport ko‘chasi 17-uy,
202A-xona
Tel: (+99899) 998-01-42
e-mail: info@al-fargoniy.uz

FARG’ONA - 2024 YIL

Jurnal quyidagi bazalarda indekslanadi:

Google Scholar · zenodo · ORCID · CYBERLENINKA · WORLD of JOURNALS · Directory of Research Journals Indexing

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

BULUTLI TEXNOLOGIYALARDA KIBERXAVFSIZLIK TAMINLASHDA CASB YECHIMLARI

Zulunov Ravshanbek Mamatovich,
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali f.-m.f.n, dotsent,

Samatova Zarnigor Nematovna,
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali 1-bosqich magistranti

Annotatsiya. Ushbu maqolada bulutli texnologiyalarda kiberxavfsizlik sohasidagi zamonaviy muammolar, axborot xavfsizligini ta'minlashda CASB sinfi yechimlari, bulutli xizmatlardan foydalanish auditi, ma'lumotlar xavfsizligi, tahdiddan himoya qilish, korporativ standartlarga muvofiqligi usullari ko’rib chiqilgan.

Kalit so‘zlar: kiberxavfsizlik, CASB yechimlari, bulutli hisoblash, axborot xavfsizligi.

Kirish. Bugungi kunda odam bir tugmani bosish orqali istalgan shakldagi ma'lumotlarni yuborishi va qabul qilishi mumkin: elektron pochta, audio yoki video, lekin u o'z ma'lumotlarining identifikatori hech qanday ma'lumot sizib chiqmasdan boshqa shaxsga qanchalik xavfsiz uzatilishi yoki xavfsiz tarzda uzatilishi haqida hech o'ylab ko'rganmi? Javob kiberxavfsizlikda. Bugungi kunda Internet kundalik hayotda eng tez rivojlanayotgan infratuzilma hisoblanadi. Hozirgi texnik sharoitda ko'plab yangi texnologiyalar inson qiyofasini o'zgartirmoqda. Ammo bu yangi texnologiyalar tufayli biz shaxsiy ma’lumotlarimizni yetarli darajada himoya qila olmaymiz va shu sababli bugungi kunda kiberjinoyatlar har kuni ortib bormoqda. Bugungi kunda jami tijorat tranzaktsiyalarining 60 foizdan ortig'i onlayn tarzda amalga oshiriladi, shuning uchun bu soha shaffof va yaxshiroq tranzaktsiyalar uchun yuqori sifatli xavfsizlikni talab qiladi. Shunday qilib, kiberxavfsizlik eng so'nggi muammoga aylandi. Kiberxavfsizlik doirasi faqat IT-sanoatdagi axborot xavfsizligi bilan cheklanib qolmaydi, balki kibermakon kabi boshqa sohalarga ham taalluqlidir.

Adabiyotlar tahlili va metodlar. Hatto bulutli hisoblash, mobil hisoblash, elektron tijorat, internet-banking va boshqalar kabi eng yangi texnologiyalar ham yuqori darajadagi xavfsizlikni talab qiladi. Ushbu texnologiyalar inson haqidagi nozik ma'lumotlarni o'z ichiga olganligi sababli, ularning xavfsizligi majburiydir. Kiberxavfsizlikni yaxshilash va muhim axborot infratuzilmalarini himoya qilish har bir mamlakat xavfsizligi va iqtisodiy farovonligi uchun muhim ahamiyatga ega. Internet xavfsizligini yaxshilash (va Internet foydalanuvchilarini himoya qilish) yangi xizmatlarni rivojlantirish hamda davlat siyosatining ajralmas qismiga aylandi [1]. Kiberjinoyatlarga qarshi kurash kompleks va xavfsizroq yondashuvni talab qiladi. Texnologik chora-tadbirlarning o‘zi jinoyatchilikning oldini ololmasligini hisobga olsak, huquqni muhofaza qiluvchi idoralar kiberjinoyatlarni samarali tekshirish va ta’qib qilish imkoniyatiga ega bo‘lishi juda muhim. Bugungi kunda ko'plab mamlakatlar va hukumatlar ba'zi muhim ma'lumotlarning yo'qolishining oldini olish uchun kiberxavfsizlik bo'yicha qat'iy qonunlarni joriy qilmoqdalar. Har bir inson ushbu kiberxavfsizlik bo'yicha o'qitilishi va o'zini bu o'sib borayotgan kiberjinoyatlardan qutqarishi kerak.

Raqamli transformatsiya davriga qadam qo‘yganimiz sari biznes tub o‘zgarishlarni boshdan kechirmoqda. Oldingi modellar va biznes jarayonlari samarasiz bo'lib qoladi, eski aloqa usullari ishlamaydi. Har bir xodim ishda, shu jumladan tashkilotdan tashqarida faol foydalaniladigan tobora ko'proq

shaxsiy gadjetlarga ega. Ishlatilgan qurilmalar turi va geolokatsiyasidan qat’i nazar, xodimlarning samarali mehnatini ta’minlash uchun Office 365, Google Apps, Salesforce, Github, Microsoft Azure, Amazon Web Services va boshqalar kabi bulutli ilovalar qo‘llaniladi. Ushbu o‘zgarishlar tufayli tarmoq perimetrida “loyqalanish” yoki “parchalanish” sodir bo'ladi.

Raqamli transformatsiya va ma'lumotlarni bulutli xizmatlarga ko'chirish:

Gartner va Forrester Wave yetakchi tahliliy agentliklari ma’lumotlariga ko‘ra, bulutli xizmatlar 2018-yilda korporativ IT-byudjetlarining 45% dan ortig‘ini tashkil qiladi.2020-yilga kelib SaaS dasturiy ta’minoti xarajatlari 75 milliard dollarga oshadi. Endi ortga qaytish yo‘q. Savol shundaki, tashkilotlar yangi raqamli dunyoda o'z ma'lumotlarini qanday himoya qilishlari mumkin.

Nega uzoqqa borish kerak? Masalan, bir nechta oddiy savollarga javob bera olasizmi? Ishonchim komilki, agar siz ilgari o'zingizga bunday savollarni bermagan bo'lsangiz, ularga berilgan javoblar qiziqarli fikrlarni uyg'otadi.

- Kompaniyangiz xodimlari qanday bulutli ilovalardan foydalanadilar?
- Bunday ilovalardan foydalanish qanday nazorat qilinadi?
- Ushbu ilovalardan foydalanish xavfi baholanadimi?

Bunday savollarga javob xavfsizlik vositalarining yangi sinfining paydo bo'lishiga olib keldi, ularsiz yaqin kelajakda zamonaviy kompaniyalarning ishlashini tasavvur qilish qiyin bo'lishi mumkin.

Kiberxavfsizlikka yangi yondashuvlar. Cloud Access Security Broker (CASB) yechimlari:

An'anaviy axborot xavfsizligi vositalari, masalan, maxfiy ma'lumotlar sizib chiqishini himoya qilish (DLP), yangi avlod xavfsizlik devorlari (NGFW, UTM), tajovuzdan himoya qilish vositalari (IPS) va boshqalar dastlab korxona tarmog'ining perimetrini himoya qilish uchun yaratilgan va ularda mutlaqo himoyasizdir. Xodimlar dunyoning istalgan nuqtasida joylashgan mobil telefonlar va noutbuklardan bulutli xizmatlar orqali hujjatlarni almashtirganda, "loyqa" perimetr shartlari. Ushbu ehtiyojni qondirish uchun CASB (Cloud Access Security Broker yoki bulutli xavfsiz kirish brokeri) deb nomlanuvchi maxsus texnologiya mavjud.

Shadow IT (shadow IT) - IT bo'limi tomonidan boshqarilmaydigan IT yechimlari. Deyarli barcha bulutli ilovalarni Shadow IT deb tasniflash mumkin, chunki... kompaniya xodimlari IT mutaxassislari ishtirokisiz turli xizmatlardan foydalanadilar. Shadow IT bilan bog'liq manbalar zararli bo'lishi shart emas. Bo'limlar ko'pincha bulut xizmatlaridan qonuniy maqsadlarda, jumladan, jamoa samaradorligini oshirish uchun foydalanadilar. Kompaniya bo'ylab foydalaniladigan bulutli ilovalarning ko'rinishini olish tashkilot foydalanuvchilari va ma'lumotlarini himoya qilishning kalitidir.

Aksariyat kompaniyalar o'z xodimlarining o'nga yaqin bulutli ilovalardan foydalanishiga ishonishadi, lekin aslida ularning soni o'rtacha yuzdan oshadi. Eng mashhur kompaniyalar, masalan, Amazon, Microsoft, Google, Adobe, Salesforce VMware va boshqalar xavfsizlik masalasiga jiddiy yondashadi. Ammo biznes nuqtai nazaridan juda qulay bo'lgan boshqa xizmatlar ham mavjud, ammo ularning xavfsizlik darajasi zarar ko'radi. Ko'pgina yosh kompaniyalar tez o'sadi yoki sekin o'ladi tamoyiliga muvofiq rivojlanadi; ularning asosiy vazifasi foydalanuvchilarga qulay, funktsional xizmatni taqdim etishdan iborat bo'lib, ular barcha kuchlarini yangi funksiyalarni qo'shish yoki foydalanuvchi interfeysini optimallashtirishga bag'ishlaydilar. Shu bilan birga, o'z mahsulotlarining tegishli darajada xavfsizligini ta'minlash uchun vaqt qolmaydi. Eng keng tarqalgan xavflarga quyidagilar kiradi:

- Ishlab chiqaruvchi tomonidan foydalanuvchi ma'lumotlari va hisob ma'lumotlarini xavfsiz saqlash;
- Yomon hisob, rol va kirish boshqaruvi;
- Xizmatlarning nomuvofiqligi, DDoS hujumlariga nisbatan zaiflik;
- Bulutli xizmat ko'rsatuvchi provayder infratuzilmasidagi zaifliklar, zamonaviy axborot xavfsizligi vositalarining yo'qligi;

- Ilovani ishlab chiqishda zaif texnologiyalardan foydalanish.

CASBning asosiy funktsiyalaridan biri kompaniyada foydalaniladigan barcha bulut xizmatlarini aniqlash, ularning har biridan foydalanish xavfini baholash va eng zaif bo'lganlarini blokirovka qilish to'g'risida qaror qabul qilishda yordam berishdir. Lekin bu CASB sinfi yechimlari qodir bo'lgan hamma narsa emas. Boshqa asosiy xususiyatlar haqida keyingi bo'limda gaplashamiz.

CASB sinfi yechimlarining funksionalligini to‘rtta asosiy blokga bo‘lish mumkin:

- Bulutli xizmatlardan foydalanish auditi;
- Ma'lumotlar xavfsizligi;
- Tahdiddan himoya qilish;
- Regulyatorlar va korporativ standartlarga muvofiqligi.

Bulutli xizmatlardan foydalanish auditi:

Biznes uchun strategik muhim vazifa bulutli xizmatlar bilan o'zaro hamkorlikning shaffofligidir. Proksi-serverlar, xavfsizlik devorlari va DNS jurnallari kabi an'anaviy tarmoq xavfsizligi vositalari faqat ba'zi asosiy ma'lumotlarni taqdim etishi mumkin. Biroq, faqat maxsus CASB yechimi zamonaviy davrda qo'llaniladigan 10 000 dan ortiq ilovalarning to'liq ko'rinishi va batafsil tahlilini ta'minlaydi.

Nega bulutli ilovalardan foydalanishning shaffofligi va tahlili zarur?

- Shadow IT Detection. IT mutaxassislariga ular foydalanadigan bulut ilovalari va ulardan foydalanadigan foydalanuvchilar haqida tushuncha beradi.
- Potentsial xavfli bulutli ilovalarni aniqlash. Xavfsizlik xodimlari uchun zaif va soxta bulutli ilovalarni aniqlash va ularni kompaniya xodimlari foydalanishi uchun nomaqbul ilovalar ro'yxatiga qo'shish mumkin bo'ladi.
- Bulutli xizmatlarga kirishni taqiqlash va ruxsat berish. Rasmga ega bo'lgach, IT foydali bulut xizmatlariga ruxsat berish va xavfli ilovalarni rad etish uchun kirish siyosatini qo'llashi mumkin.
- Normativ muvofiqlik. Xavfsizlik xodimlari foydalanilayotgan bulut xizmatlarini kuzatishi va ulardan foydalanish me'yoriy talablarga muvofiqligini ta'minlashi mumkin.

CASB klassi yechimlari bulutli xizmatlarda ma'lumotlar himoyasini ta'minlaydigan funksionallikka ega. Muayyan qurilmalardan ma'lum xizmatlarga kirish huquqlarini boshqarish, shuningdek, muhim ma'lumotlarga kirish huquqlarini cheklash vositalari mavjud. Ko'pgina etuk CASB yechimlarida shubhali harakatni erta aniqlashga yordam beradigan o'rnatilgan foydalanuvchi xatti-harakatlari tahlili (UEBA) mavjud.

Bundan tashqari, CASB maxfiy ma'lumotlarni saqlash va uzatishni aniqlash va tahlil qilish imkonini beruvchi ma'lumotlarni turkumlashtirish funksiyasiga ega, bu asosan bulutda ma'lumotlar yo'qolishining oldini olish (DLP) yechimidir. Qochqinlarni himoya qilishning ilg'or funksiyalarini olish uchun uchinchi tomon DLP tizimlarini CASB bilan birlashtirish mumkin.

Nihoyat, CASB bulutga yuborilgan maxfiy ma'lumotlarni anonimlashtirish va shifrlash imkonini beradi. To'liq yoki tanlab shifrlashni qo'llash va turli xil algoritmlardan foydalanish mumkin.

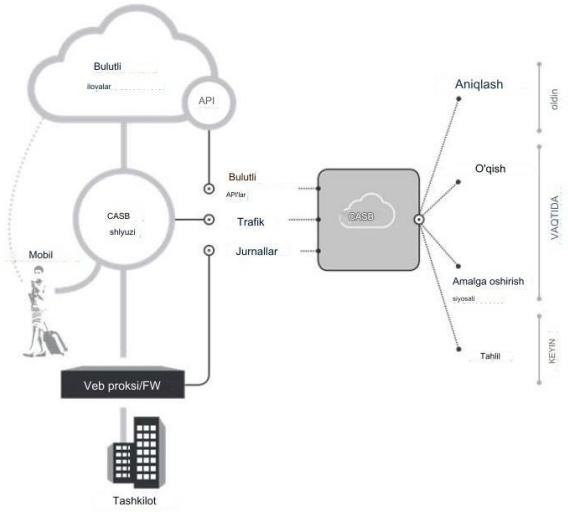
Korxona darajasidagi bulut ilovalari yaxshi himoyalangan. Va tajovuzkorlar tomonidan ishlatiladigan asosiy hujum vektori foydalanuvchi hisob ma'lumotlarini buzish va shu tariqa ma'lumotlarga kirish huquqiga ega bo'lishdir. Bundan tashqari, tajovuzkorlar zararli dasturlarni tarqatish va tashkilot infratuzilmasiga maqsadli hujumlar uyushtirish imkoniyatiga ega.

Tahdidlardan himoya qilish uchun CASB o'zining arsenalida xulq-atvor tahlili, virusga qarshi skanerlash, xatti-harakatlar namunalarini o'rnatish uchun mashinani o'rganishdan foydalanish va bulutli xizmat ko'rsatuvchi provayderlarning real vaqtda tahdidlar ma'lumotlaridan foydalanish kabi turli xil oldini olish usullariga ega.

Tashkilotning bulutga qisman o'tishi bilan ham, shaxsiy va korporativ ma'lumotlar xavfsizligini ta'minlaydigan ichki va tashqi standartlarga rioya qilish muhim bo'lib qolmoqda. Kompaniyada qo'llaniladigan barcha bulutli ilovalarning ko'rinishi va nazorati tufayli bulut xavfsizligining joriy holatini baholash,

shuningdek, uni zarur standartlarga muvofiqlashtirish uchun kirish siyosatidan foydalanish mumkin bo'ladi.

Natijalar. CASB arxitekturasi va ishlash tamoyili: CASB yechimlari ko'pincha bulutda joylashtiriladi va API va/yoki proksi-serverlar orqali foydalanuvchilar va ilovalarning o'zaro ta'sirini nazorat qiladi. Mahalliy va gibrid rejimlardan ham foydalanish mumkin.



Rasm 1. CASB yechimi arhitekturasi.

CASB joylashtirish arxitekturasini tanlash ma'lum bir tashkilotning infratuzilmasi va ehtiyojlariga bog'liq. Qaysi variant yaxshiroq ekanligiga aniq javob yo'q. Shu bilan birga, yetakchi tahlil agentliklari gibrid yondashuvni funksionallik nuqtai nazaridan eng to‘liq deb ta’kidlaydilar.

Deyarli har bir yirik sotuvchi o'z portfelida ushbu sinfning yechimiga ega. Rahbarlar orasida yetakchi tahlil agentliklari McAfee (Skyhigh Networks), Netskope va Symantec kompaniyalarini ajratib ko'rsatishadi. Bundan tashqari, Cisco, Forcepoint, Microsoft, Oracle, Palo Alto'dan CASB mavjud.

Muayyan tashkilot uchun eng mos bo'lgan echimni tanlashda quyidagi masalalarni ko'rib chiqish tavsiya etiladi:

Bulutli ilovalarni kashf qilish:

- Ilovaning xavfsizlik reytingini hisoblash uchun qancha xavf atributlaridan foydalaniladi? Xavfli atributlarga og'irliklarni qo'lda belgilash mumkinmi?
- Yechim xavflarni baholashning avtomatlashtirilgan hisobotlarini taqdim etadimi?
- Veb-proksi-server yoki xavfsizlik devori bilan integratsiya orqali kiruvchi bulutli ilovalarni bloklash mumkinmi?

Kerakli siyosatlarning mavjudligi:

- Taqiqlangan va ruxsat etilgan ilovalar uchun xavfsizlik siyosatini sozlash mumkinmi?
- Yechim tashkilot perimetri tashqarisida joylashgan mobil qurilmalar va noutbuklardan bulut xizmatlaridan xavfsiz foydalanishni qo‘llab-quvvatlaydimi?
- Foydalanuvchi nomi, guruh, qurilma, joylashuv, brauzer yoki foydalanuvchi agenti kabi kontekst va kontentga asoslangan foydalanuvchi harakatlariga batafsil siyosatlarni qo'llash mumkinmi?
- Bir nechta bulutli ilovalarda izchil siyosatlarni amalga oshirish mumkinmi?

Joylashtirish:

- Yechim xavfsizlik investitsiyalaridan qayta foydalanishni maksimal darajada oshirish uchun mavjud veb-proksi yechimlari bilan mos keladimi?
- Tizim uchun rolga asoslangan kirish modeli bormi?

Ma'lumotlarni boshqarish:

- Tizimda ma'lumotlarni yo'qotishdan himoya qilish (DLP) funksiyasi bormi?
- Uchinchi tomon DLP yechimlari bilan integratsiya qilish mumkinmi?
- Muntazam ifodalar va kontekstual tahlil kabi ma'lumotlarni tasniflash usullari qo'llab-quvvatlanadimi?
- Yechim tranzit, foydalanish va bulutda saqlangan vaqtda tokenizatsiya va ma'lumotlarni shifrlash qobiliyatini qo'llab-quvvatlaydimi?

Tahdidni aniqlash:

- Yechimda shubhali faoliyatni aniqlash uchun foydalanuvchi xatti-harakatlarini tahlil qilish (UEBA) funksiyasi bormi?

- Yechim bir qarashda zararli faoliyatni tushunishga yordam beradigan ilg'or vizualizatsiyani ta'minlaydimi?
- Yechim o'rnatilgan zararli dasturlarni aniqlash funksiyasiga egami?
- Yechim uchinchi tomon hujumlaridan maqsadli himoya (ATP) yechimlari bilan integratsiyani qo'llab-quvvatlaydimi?

Foydalanish qulayligi va interfeysi:

- O'rnatish va boshqarish uchun yechim qanchalik murakkab;
- Foydalanuvchi interfeysi qanchalik intuitiv;
- Yakuniy foydalanuvchilar uchun kechikishlar yoki noqulayliklar bormi;
- Agar CASB yechimi muvaffaqiyatsiz bo'lsa, foydalanuvchilar bulutli ilovalarga kira oladimi;
- Masshtablilik: Yechim qancha foydalanuvchi va tranzaktsiyalarni qo'llab-quvvatlaydi.

Xulosa. Kompyuter xavfsizligi keng ko'lamli mavzu bo'lib, dunyo tobora o'zaro bog'lanib borayotgani va muhim tranzaktsiyalarni amalga oshirish uchun tarmoqlardan foydalanilgani sababli tobora muhim ahamiyat kasb etmoqda. Axborot xavfsizligi kabi kiberjinoyatlar ham yil sayin turli yo'llarni bosib o'tishda davom etmoqda. Rivojlanayotgan va buzg'unchi texnologiyalar, shuningdek, har kuni kashf etilayotgan yangi kiber vositalar va tahdidlar tashkilotlarni nafaqat o'z infratuzilmasini himoya qilishda, balki buning uchun yangi platformalar va razvedka talab qilishda ham qiyinchilik tug'dirmoqda. Kiberjinoyat uchun mukammal yechim yo'q, lekin biz kibermakonda xavfsiz va xavfsiz kelajakka ega bo'lish uchun uni minimallashtirishga harakat qilishimiz kerak.

CASB sinfi yechimlari bulutli ilovalardagi ma'lumotlarni himoya qilishga qaratilgan. Ular Shadow IT-ni aniqlash, kirish, trafik va ma'lumotlar harakatlarini nazorat qilish, ruxsat etilgan va taqiqlangan bulut xizmatlaridan foydalanish bo'yicha aniq tahlillarni taqdim etish imkoniyatiga ega. CASB yechimlari ma'lumotlar sizib chiqishiga qarshi kurashish imkonini beradi, foydalanuvchi xatti-harakatlarini tahlil qilish vositalariga ega va uzatilgan ma'lumotlarni anonimlashtirish va shifrlash imkoniyatiga ega. Zararli dasturlardan va ruxsatsiz kirishdan himoya qilish funksiyasi ham mavjud.

CASB yechimlari uchun jahon bozori hali to'liq shakllanmagan, biroq unda o'z mahsulotlarida eng to'liq funksionallikni ta'minlaydigan aniq yetakchilar allaqachon mavjud. Hozircha ushbu sinfning mahalliy echimlari yo'q, ammo 2019 yilda bo'lajak relizlar haqida allaqachon ma'lumotlar mavjud. Kundalik hayotimizda turli xil bulutli xizmatlarning rivojlanishi va ulardan foydalanishning keskin o'sishini sezmaslik qiyin va ishonch bilan aytish mumkin. Rossiya bozorida CASBga qiziqish juda yuqori bo'ladi.

Adabiyotlar:

1. Eric Andrews, Gerry Grealish, Rehan Jalil. Securing Cloud Applications & Services - An executive guide. Symantec Corp. 2017.
2. Cybercrime [Электронный ресурс] // URL: https://en.wikipedia.org/wiki/Cybercrime.
3. VV Byts', RM Zulunov. Specification of matrix algebra problems by reduction. Journal of Mathematical Sciences. T. 71, 2719–2726 (1994).
4. https://www.anti-malware.ru/analytics/Market_Analysis/cloud-access-security-broker
5. https://www.gartner.com/it-glossary/cloud-access-security-brokers-casbs/
6. https://www.esecurityplanet.com/products/top-casb-vendors.html
7. https://en.wikipedia.org/wiki/Cloud_access_security_broker
8. R. Zulunov. Pythonda neyron tarmoqni qurish va bashorat qilish. Al-Farg'oniy avlodlari, 2023, 1/4, c. 22-26.
9. Р.Зулунов, А. Каюмов. Искусственный интеллект - от мифологии до машинного обучения. Proceedings of International Educators Conference. Том 1, 2, с. 25-30.
10. Р.Зулунов, А.Абдукодиров. Этические и правовые аспекты внедрения искусственного интеллекта. Research and implementation, 2023, 1/6, с. 14-20.

11. Р.Зулунов, Б.Солиев. Использование Python для искусственного интеллекта и машинного обучения. Al-Farg'oniy avlodlari, 2023, 1/3, с. 18-24.
12. R.Zulunov. Sun'iy intellektni axloqiy va huquqiy muammolari. Journal of technical research and development. 2023, 1/1, с. 120-124.
13. Р.Зулунов, Д.Ирматова. Использование технологий искусственного интеллекта. Журнал интегрированного образования и исследований. 2022, 1/6, с. 53-56.
14. Р. Зулунов, А.Горовик. Методика преподавания визуального программирования для детей. Цифровой регион: опыт, компетенции, проекты: сборник статей Международной научно-практической конференции. – Брянск: БрГИТУ, т.1, с. 193-197.
15. Р. Зулунов, А.Горовик. Внедрение технологий искусственного интеллекта, нравственные и правовые нормы. Conference on Digital Innovation: "Modern Problems and Solutions", 2023.