RAQAMLI IQTISODIYOT VA AXBOROT TEXNOLOGIYALARI
2025
№2
aprel-iyun
http://dgeconomy.tsue.uz/
ILMIY ELEKTRON JURNAL

BANKLARDA MOSLASHTIRILGAN DLP ALGORITIMINI QO‘LLASH

Matyakupova Madina Quzibay qizi
Toshkent davlat iqtisodiyot universiteti, Axborot tizimlari va texnologiyalari kafedrasi o‘qituvchisi
m.matyakupova@tsue.uz

Annotatsiya
Ushbu maqolada banklarning tashkiliy tuzilishi ko‘rib chiqilgan, kredit-moliya muassalarida axborot xavfsizligini ta’minlashga oid standartlar va qonun hujjatlari, kredit-moliya muassasalari xavfsizligiga taxdidlar va ulardan himoyalanish masalalari, tizim zaifliklari va ularning xalqaro miqyosdagi indekslari tahlil qilgan. Axborot xavfsizligining konseptual modeli asosida kredit-moliya muassasalarining tahdid modeli ishlab chiqilgan. Tahdid modeli asosida kredit-moliya muassasalarida ma’lumotlarni sirqib chiqishidan himoyalash usul va algoritmlari o’rganilgan va axborotni sirqib chiqishdan kelib chiqadigan harajatlarni baholash amalga oshirilgan. Shuningdek, bank axborot tizimining o’ziga xos xususiyatlariga moslashtirilgan DLP algoritmi ishlab chiqilgan va uni qo’llash bo’yicha erishilgan samaradorlik aniqlangan.

Аннотация
В данной статье рассмотрена организационная структура кредитно-финансовых учреждений, проанализированы стандарты и законодательство, касающиеся обеспечения информационной безопасности в кредитно-финансовых учреждениях, угрозы безопасности кредитно-финансовых учреждений и вопросы защиты от них, системные уязвимости и их индексы на международном уровне. На основе концептуальной модели информационной безопасности разработана модель угроз кредитно-финансовых учреждений. На основе модели угроз были изучены методы и алгоритмы защиты от утечки информации в кредитно-финансовых учреждениях, проведена оценка издержек от утечки информации. Также разработан алгоритм DLP, адаптированный под специфику банковской информационной системы, и определена достигнутая эффективность его применения.

Annotation

This article examines the organizational structure of credit and financial institutions, analyzes the standards and legislation related to the provision of information security in credit and financial institutions, taxids and protection issues on the security of credit and financial institutions, system vulnerabilities and their indexes at an international level.
On the basis of the conceptual model of Information Security, a threat model of credit and financial institutions has been developed. On the basis of the threat model, methods and algorithms for protecting data from slippage have been studied in credit and financial institutions, and an assessment of the costs arising from information slippage has been carried out. Also, a DLP algorithm has been developed, adapted to the specifics of the banking information system, and the achieved efficiency in its application has been determined.

Kalit so‘zlar
Kredit kartalari, elektron raqamli imzo, moliyaviy kriptografiya, blockchain texnologiyalari, DSA, ECDSA, DLP sistemasi, elektron tijorat, elektron pul.

Ключевые слова
кредитные карты, цифровая подпись, финансовая криптография, технология блокчейн, DSA, ECDSA, система DLP, электронная коммерция, электронные деньги.

Keywords
credit cards, electronic digital signature, financial cryptography, blockchain technologies, DSA, ECDSA, DLP system, e-commerce, e-money.

Kirish

O‘zbekiston Respublikasi Prezidentining 2022 yil 28 yanvardagi PF 60-sonli farmoni bilan tasdiqlangan “2022–2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida”da “Shaxsiy va sir saqlanishi lozim bo‘lgan ma’lumotlarni Internet tarmog‘ida oshkor qilish bilan bog‘liq daxlsizlik huquqi buzilishining oldini olish” va “Kiberjinoyatchilikning oldini olish tizimini yaratish” bilan bog’liq bo‘lgan bir qator vazifalar belgilangan.

Ko‘pincha sirqib chiqishlar ichkarida sodir bo‘ladi. Manbalar ataylab yoki tasodifan ma'lumotni tegishli bo‘lmagan shaxslarga taqdim etadigan xodimlardir. Hackerlar juda kam hollarda tahdid manbasi bo‘lib hizmat qilmoqdalar. Sababi, ko‘pchilik xakerlar buzib kirishni amalga oshirishlari uchun kompaniya ichidagi kimdandir kirish huquqiga ega bo‘lishlari kerak. Banklar uchun biznesning uzluksizligi muhim ahamiyatga ega. Shuning uchun, DLP tizimi uchun biznes jarayonlarini buzmasdan yoki to‘xtatmasdan amalga oshirish qobiliyatini ta’minlashi uchun DLP texnologiyalaridan foydalanish talab etiladi.

Mavzuga oid adabiyotlar tahlili

Kredit-moliya muassalarida, xususan bank sohasida axborot xavfsizligini ta’minlash bo‘yicha ko‘plab taniqli xorijiy olimlar, masalan, R.Debar, S.Hazari, M.Whitman, B.Carrier, D.Anderson, A.Vnukov, V.Vasilyev, T.Andriyanova

tomonidan o‘rganib chiqilgan. Bundan tashqari ular krdit-moliya tizimlarida mavjud zaifliklar tahlili, xavfsizlik bo’yicha Bazel standartini qo’llash bo’yicha, shuningdek bank axborot tizimini xavfsizlgini ta’minlashning samarali modellari va usullarini ishlab chiqish bo‘yicha asosiy xarakterga ega bo‘lgan takliflarni qayd etib o‘tishgan.

Tadqiqot metodologiyasi

Ushbu maqolada axborotni sirqib chiqishdan himoyalash, axborot xavfsizligni ta’minlashning konseptual modeli, kredit-moliya muassasalarining tahdid modellarini qurish nazariyasi, axborot xavfsizligi usullari, informatika va matematika asoslari, ehtimollik nazariyasi va matematik statistika, tizim va tizimli tahlil usullari, algoritmlash usullaridan foydalanilgan.

Tahlil va natijalar

Kredit-moliya muassasalarining tashkiliy tuzilishi.

Moliya-kredit tashkiloti - kredit berish, depozit qo‘yish, joriy hisobvaraqlarni yuritish, valyuta va qimmatli qog‘ozlarni sotib olish va sotish, moliyaviy xizmatlar ko‘rsatish va boshqalar bo‘yicha moliyaviy operatsiyalarni amalga oshirishga vakolatli davlat yoki xususiy, tijorat tashkiloti. Kredit tashkilotlariga omonat kassalari, banklar, kooperativlar, mikromoliya tashkilotlari va boshqalar kiradi.

Iqtisodiyotni samarali boshqarish uning muhim sub’ekti bo‘lgan banklar faoliyatini o‘rganishni, ularning ishlash usullari, funktsiya va operatsiyalarini bilishni taqazo qiladi.

Bank kengashi omonatchilar va aktsiyadorlarni himoya qilish maqsadida bank faoliyatini, shu jumladan, kreditlash va mablag‘larni investitsiyalashning to‘g‘riligini nazorat qilish;

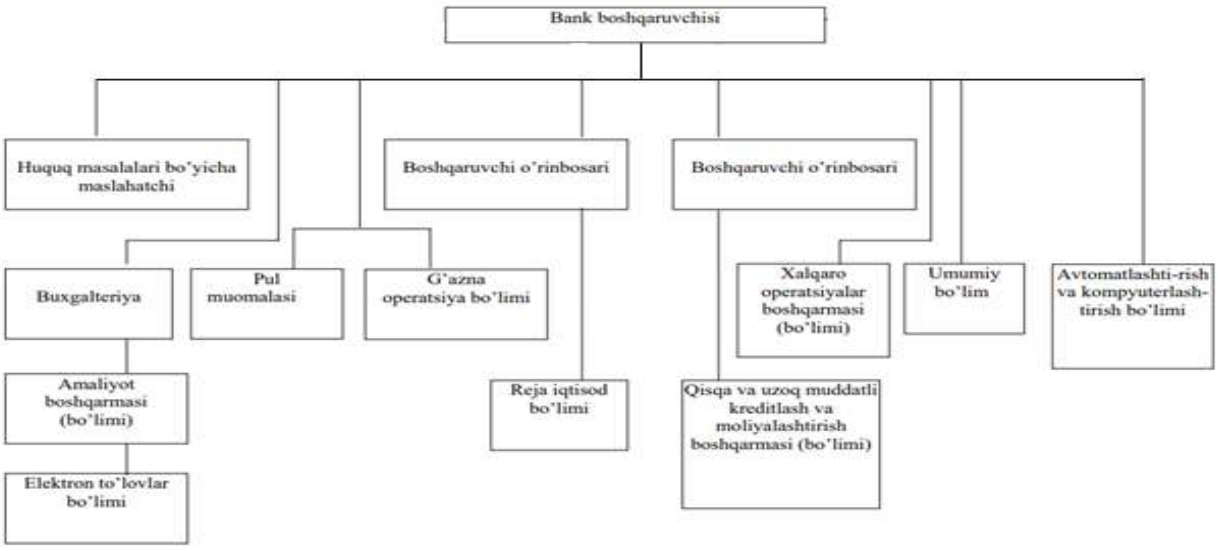
bank rahbarlarini ishga tayinlash va ishdan bo‘shatish;

bank kapitalining bir tekis o‘sib borishini ta’minlab turish;

bank siyosatini ishlab chiqish;

qonun hujjatlariga rioya qilishni ta’minlash va boshqa vazifalarni amalga oshiradi;

Tijorat banklarning tashkiliy tuzilishini Respublika aktsiyadorlik tijorat banki misolida quyidagi chizmada ko‘rish mumkin.



1-rasm. Bankning tashkiliy tuzilishi

Yuqorida keltirilgan bankning tashkiliy tuzilishi aksariyat banklar uchun o‘xshash bo‘lib tijorat banklarining joylanishi o‘rni, xizmat ko‘rsatadigan mijozlarning faoliyati xususiyatlaridan kelib chiqib ba’zi bir o‘zgarishlar bo‘lishi mumkin.

Kredit-moliya muassasalarida DLP tizimini qo`llash.

Ko‘pincha sirqib chiqishlar ichkarida sodir bo‘ladi. Manbalar ataylab yoki tasodifan ma'lumotni tegishli bo‘lmagan shaxslarga taqdim etadigan xodimlardir. Hackerlar juda kam hollarda tahdid manbasi bo‘lib hizmat qilmoqdalar. Sababi, ko‘pchilik xakerlar buzib kirishni amalga oshirishlari uchun kompaniya ichidagi kimdandir kirish huquqiga ega bo‘lishlari kerak.

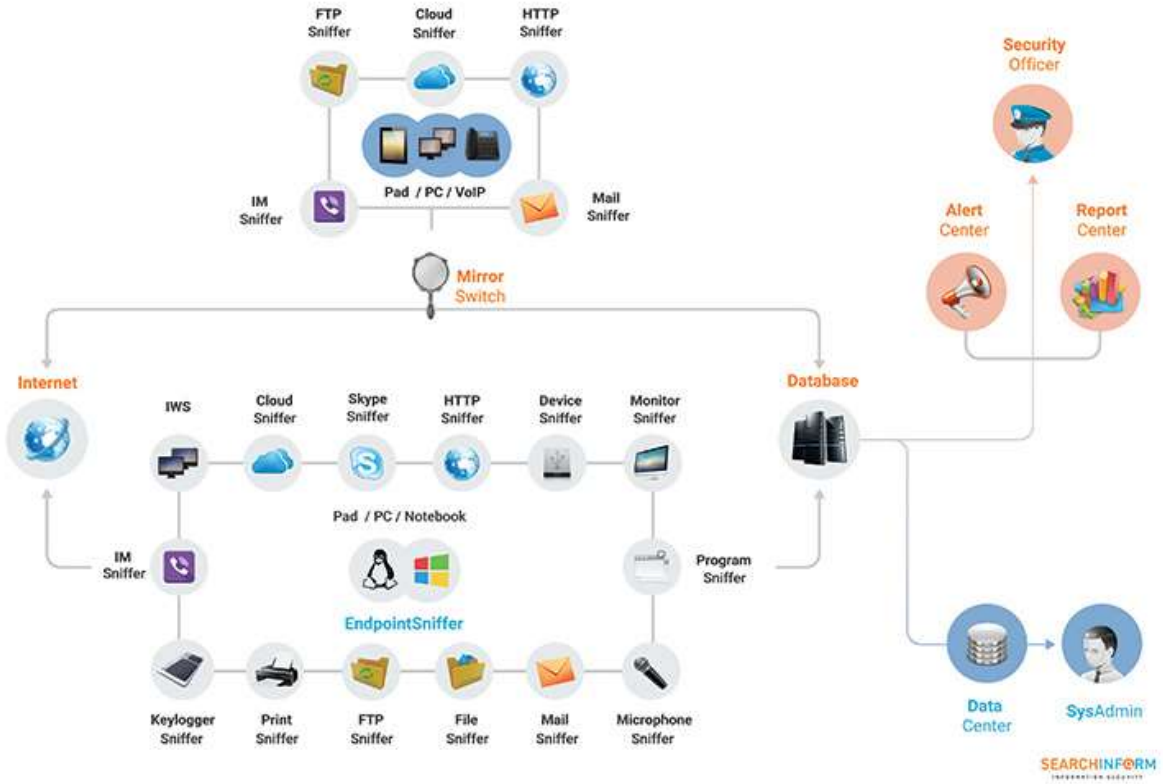
Ma'lumotlar asosan ochiq manbalardan olinadi. Shuning uchun, bu statistikaga faqat matbuotga sirqib chiqqan rezonansli holatlar kiradi. Kompaniyalar o‘z hodisalarining statistikasini yo umuman yuritmaydilar yoki taqdim etmaydilar. Ko‘p hodisalar ataylab reklama qilinmaydi. Biroq, biz biror narsaga tayanishimiz kerak.

DLP texnologiyasi uzatish kanallarini boshqarish imkonini beradi: ularda qanday ma'lumotlar aylanayotganini kuzatib borish va kerak bo‘lganda ba'zilarini blokirovka qilish mumkiin. Albatta, u juda ko‘p maxfiy ma'lumotlar bilan ishlaydigan tashkilotlar, jumladan banklarni qiziqtiradi.

Banklar tizimning yagona boshqaruv markaziga ega bo‘lishidan manfaatdor. Qoida tariqasida, DLP tizimlari bir nechta modullardan iborat bo‘lib, ularning har biri o‘z funktsiyalarini bajaradi. Biroq, har bir tizimda barcha modullar uchun yagona boshqaruv markazi mavjud emas, buni kompaniyalar noqulay deb hisoblaydi.

Moslashtirilgan DLP algoritmini qo’llash bo‘yicha olingan natijalar.

Banklarga yetkaziladigan zararning “noaniqligi” ga qaramay, yuqoridagi xolatlarni yuzaga kelish ehtimoli mavjudligining o‘zi odatda DLP tizimini sotib olish uchun asos bo‘lib xizmat qiladi. Muammo barchaga tegishli va u yildan-yilga o‘sib bormoqda.



1-rasm. Standart DLP tizimining arxitekturasi

DLP tizimining arxitekturasi ko‘p modulli. U ikki darajadagi ma'lumotlarni ushlab qoladi va tahlil qiladi: tarmoqda va xostda.

Tadqiqot natijasida axborot xavfsizligi hodisalarini tahlil qilish metodologiyasi, aniqlangan hodisalarga javob berish algoritmi, shuningdek, standart DLP tizimini Bank faoliyatining o‘ziga xos xususiyatlariga moslashtirish metodologiyasi va tartiblari ishlab chiqiladi.

Standart DLP tizimini bank ishining o‘ziga xos xususiyatlariga moslashtirish metodologiyasi quyidagi tadbirlardan iborat:

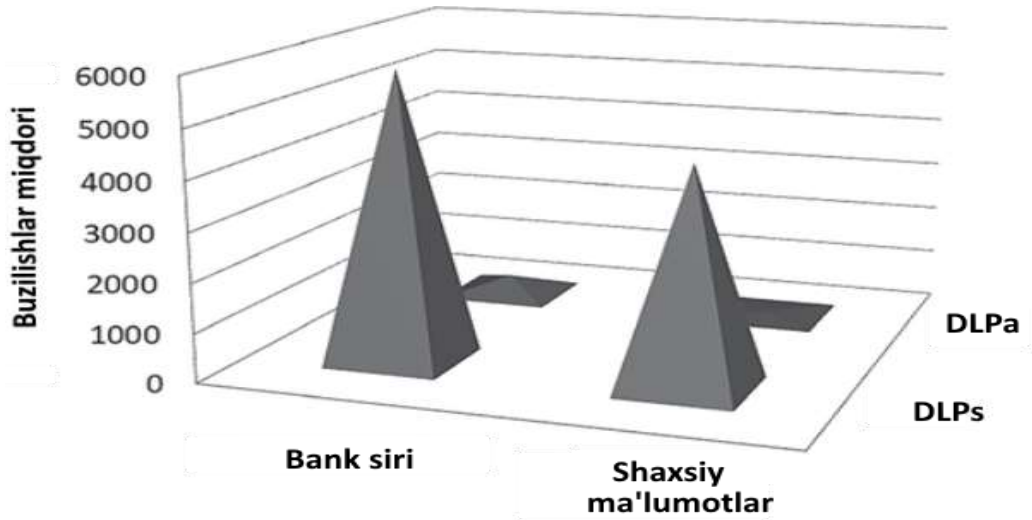
- muhim korporativ ma'lumotlarning toifalarini aniqlash,
- axborot tizimlarini tekshirish,
- joriy risklarni tavsiflash va ularni baholash,
- cheklangan ma'lumotlar bilan ishlash qoidalarini joriy etish va boshqaruv tizimini yaratish.

Standart DLP tizimining konfiguratsiyasini yangilash quyidagi tartiblarni o‘z ichiga oladi:

- a'zolik mezoniga ko‘ra Bankning maxfiy ma'lumotlarini tanlash,
- ajratib olishni sozlash,
- perimetrlarni yaratish
- bankda aniqlangan axborot xavfsizligi hodisalariga javob berish algoritmini ishlab chiqish.

To‘liq xususiyatli DLP tizimining asosiy ko‘rsatkichi, maxfiy ma'lumotlarning chiqib ketishining oldini olishdir. Biroq, bugungi kunda DLP tizimlaridan axborot xavfsizligi kompleksining elementi sifatida foydalanadigan kompaniyalarning 50% dan kamrog‘i maxfiy ma'lumotlarning sirqib chiqishi uchun DLP tizimining ishlashini “Nusxa olish” rejimidan “Bloklash” rejimiga o‘tkazgan. Bunday kompaniyalar o‘zlarining DLP tizimining nozik ma'lumotlar tasnifining to‘g‘riligiga ishonchlari komil emas va kompaniyaning biznes jarayonlarining buzilishidan qo‘rqishadi. DLP tizimining “Nusxa ko‘chirish” rejimida ishlashi maxfiy ma'lumotlarning kompaniyadan tashqariga chiqarilishiga to‘sqinlik qilmaydi, balki faqat tugallangan axborot xavfsizligi hodisalarini ko‘rsatadi. DLP tizimining ishlashini “Bloklash” rejimiga o‘tkazish muammosini hal qilish DLP yechimining moslashuv sozlamalari hisoblanadi.

Moslashuvchan DLP-tizimining natijalari. Moslashuvchan DLPa ishlashini baholash uchun ikkita hisobot yaratildi va tahlil qilindi. Birinchi hisobot DLP tizimining standart sozlamalari bo‘lgan DLP'lar uchun 7 kun davomida “Bank siri” va “Shaxsiy ma'lumotlar” ni himoya qilish ob’yektlari aniqlangandan keyin yaratildi. Ikkinchi hisobot “Bank siri” va “Shaxsiy ma'lumotlar” bir xil himoya ob’yektlari 7 kun davomida aniqlanganda, lekin DLPa uchun DLP tizimini Bank ishining o‘ziga xos xususiyatlariga moslashtirish jarayonidan so‘ng yaratilgan. Ikkita hisobot ma'lumotlari 2-rasmda ko‘rsatilgan.



	Bank siri	Shaxsiy ma'lumotlar
DLPs	5874	4401
DLPa	364	70

2-rasm. Ushlab qolingan DLP va DLPa hodisalari statistikasi

Bankdagi adaptiv DLPadan foydalanish shaxsiy ma'lumotlarni o‘z ichiga olgan ma'lumotlarni aniqlashda DLP-tizimining noto‘g‘ri ishlab ketishlarni 16 barobarga, bank sirini tashkil etuvchi ma'lumotlarni aniqlashda esa 62 baravarga qisqarishiga olib keldi. Olingan eksperimental ma'lumotlarga asoslanib, biz quyidagi o‘zgarishlarni aytishimiz mumkin:

1. Axborot oqimida maxfiy ma'lumotlarni aniqlashning aniqligi oshdi.
2. Bankda DLPa tomonidan aniqlangan axborot xavfsizligi hodisalariga javob berish tezligi oshdi.
3. Tizimni nusxa ko‘chirish rejimidan noqonuniy ma'lumotlar uzatishni blokirovka qilish rejimiga o‘tkazish imkoniyati bilan bog‘liq holda DLPa samaradorligi oshirildi.

Bankda moslashtirilgan DLP tizimidan foydalanish axborot xavfsizligi xizmati mutaxassislarining Bankdagi moslashtirilgan DLP tizimi tomonidan aniqlangan axborot xavfsizligi hodisalariga javob berish tezligini oshirish imkonini berdi, shuningdek, DLP ishini almashtirish imkonini berdi.

Xulosa

Xulosa o’rnida aytish mumkinki, banklarda axborot xavfsizligini ta’minlashga oid standartlar va qonun hujjatlari hamda kredit-moliya muassasalari xavfsizligiga taxdidlar va ulardan himoyalanish masalalari, tizim zaifliklari va ularning xalqaro miqyosdagi indekslari tahlil qilindi.

Axborotni sirqib chiqishdan kelib chiqadigan harajatlarni baholash amalga oshirildi. Shuningdek, standart DLP tizimlarida yuzaga keladigan yolg’on ishga tushishlarni bartaraf etishdan himoyalash va DLP tizimlarining samarador ishlashini ta’minlash maqsadida bank axborot tizimining o’ziga xos xususiyatlariga moslashtirilgan DLP tizimlaridan foydalanish tavsiya etildi. Tavsiya etilgan adaptiv DLP algoritmini qo’llash bo’yicha erishilgan samaradorlik ko’rsatkichlari baholandi.

Foydalanilgan adabiyotlar ro‘yxati

1. “2022 – 2026 - yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida” 28.01.2022 yildagi PF-60 sonli O‘zbekiston Respublikasi Prezidentining farmoni.

2. Axborot-Kommunikatsiya texnologiyalari sohasida loyiha boshqaruvi tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida O‘zbekiston Respublikasi Prezidentining 29.08.2017 PQ-3245-son qarori.

3. O’zbekiston Respublikasining O‘RQ-30-sonli “Avtomatlashtirilgan bank tizimida axborotni muhofaza qilish to‘g‘risida”gi Qonuni 2006-yil 6-aprel.

4. O’zbekiston Respublikasining O‘RQ-582-sonli “O‘zbekiston Respublikasining markaziy banki to‘g‘risida”gi Qonuni (yangi tahrir) , 2019-yil 11-noyabr.

5. O’zbekiston Respublikasining O‘RQ-580-sonli «Banklar va bank faoliyati to‘g‘risida»gi Qonuni. 2019-yil 5-noyabr.

6. O’zbekiston Respublikasi Prezidentining 2018-yil 8-avgustdagi PF-5505_son “Norma ijodkorligi faoliyatini takomillashtirish konseptsiyasini tasdiqlash to’g’risida”gi Farmoni.

7. Внуков, А. А. Защита информации в банковских системах: учеб. пособие для бакалавриата и магистратуры / А. А. Внуков; М.: Издательство Юрайт, 2017. – 246 с.