

KIBERJINOYATLAR ASOSIDAGI MA'LUMOTLAR STATISTIKASINI YARATISH MOSELINI ISHLAB CHIQUISH

Radjabova M.Sh
Abdullayev I
Suyunov K
Odilov O

*Muhammad al-Xorazmiy nomidagi Toshkent
axborot texnologiyalari universiteti*

Anatatsiya: *Kiberjinoyatlar internet, tarmoq va kompyuter tizimlarida yuzaga keladigan xavfli faoliyatlar va shaxslarga zarar yetkazadigan tashqi hujjatlarni olish yoki tahrirlashni o'z ichiga oladi.*

Kalit so'zlar: *global kiberjinoyatlar, kiberjinoyatchilik statistikalari, Milliy kiberjinoyatchilik indeksi, kiberjinoyat tahlili.*

Ma'lumki, XXI asr – axborot texnologiyalari asri. Biroq, bu hodisaga doimo ijobiy ob'yektiv baho berish juda qiyin, chunki ijobiy va salbiy tomonlari bor. Salbiy jihatlardan biri bu kiberjinoyatlarning ko'payishidir. Bu bir yoki bir necha shaxslar tomonidan oldindan kelishib yoki kelishuvsiz sodir etilgan qilmishdir. Bu jinoyatlar, asosan, internet va raqamli texnologiyalardan keng ma'lumotga ega bo'lgan shaxslar tomonidan o'z g'arazli maqsadlariga erishish uchun amalga oshiriladigan harakatlar majmuidir. Internetning keng tarqalishi va aloqa xizmatlarining arzonligi tovarlarni sotishdan tortib davlat xizmatlarini olishgacha bo'lgan masofaviy imkoniyatlarning o'sishiga olib keldi. Bank sektori raqamli xizmatlarni rivojlantirishda eng ilg'or hisoblanadi. U yerda elektron tranzaksiyalar soni kundan-kunga ortib bormoqda va IT tizimining yangi elementlari paydo bo'lmoqda. Kiberjinoyat - bu kompyuterlar va tarmoqlar bilan bog'liq holda sodir etiladigan jinoyatlarning bir turi. Jinoyat paytida kompyuter maqsadli qurol vazifasini bajaradi.



Bir yil ichida 1 milliardga yaqin elektron pochta xabarlarini fosh qilindi, bu har 5 internet foydalanuvchisidan 1 tasiga ta'sir ko'rsatdi.



2022 yilda ma'lumotlar buzilishi korxonalariga o'rtacha 4,35 million dollarga tushadi.



2022-yilning birinchi yarmida dunyo bo'ylab 236,1 millionga yaqin to'lov dasturlari hujumi sodir bo'ldi.



2021-yilda har 2 amerikalik internet foydalanuvchisidan 1 nafarining akkauntlari buzilgan.



Buyuk Britaniya korxonalarining 39 foizi 2022-yilda kiberhujumga uchraganini ma'lum qildi.



Taxminan 10 ta AQSH tashkiloti kiberhujumlardan sug'urta qilmaydi.



2022 yilning birinchi yarmida 53,35 million AQSh fuqarosi kiberjinoyatlardan jabrlangan.

2.11-rasm. Kiberjinoyatlar statistikasi sarlavhasi



2022-yilda bir million internet foydalanuvchisiga to'g'ri keladigan kiberjinoyat qurbonlari soni Buyuk Britaniyada 4783 taga yetgan, bu 2020-yilga nisbatan 40 foizga ko'p. 2022-yilda har bir million internet foydalanuvchisi qurbonlari soni bo'yicha keyingi eng ko'p bo'lgan mamlakat 1494 ta bilan AQSh bo'ldi, bu 2020 yilga nisbatan 13 foizga kamaygan. 2021 yilda Shimoliy Amerikadagi har 2 internet foydalanuvchisidan 1 nafari akkauntlari buzilgan.



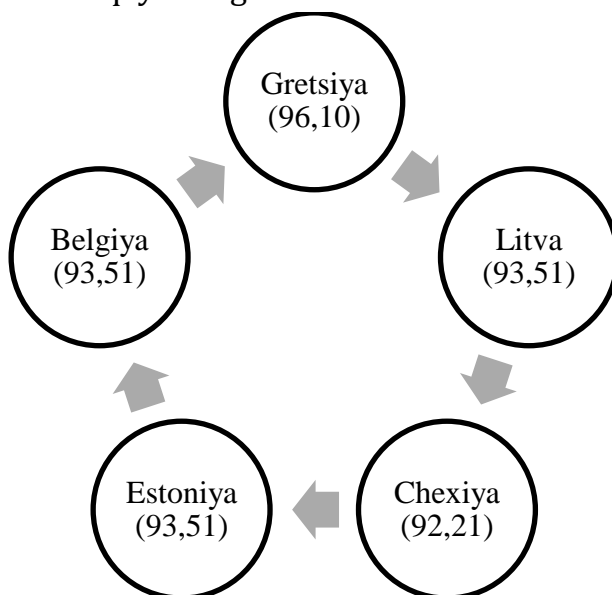
Buyuk Britaniya va AQShda boshqa mamlakatlarga nisbatan har bir million internet foydalanuvchisiga nomutanosib ravishda ko'proq kiberjinoyat qurbonlari bor - AQShda 2021 yilda keyingi eng yuqori mamlakat Kanadaga qaraganda 759% ko'proq qurbon bo'lgan. 2021 yilda dunyo bo'ylab har soatda o'rtacha 97 nafar ma'lumotlar buzilishi qurboni bo'lgan.



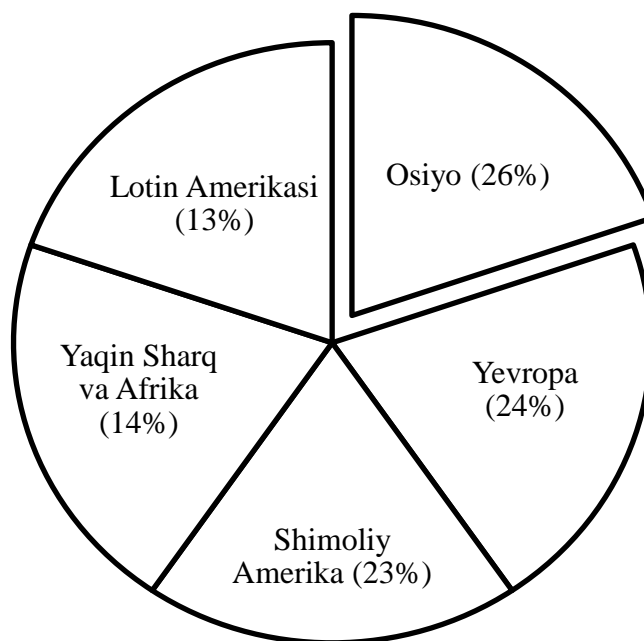
2020-2021-yillar may oylari orasida Osiyo-Tinch okeani mintaqasida kiberjinoyatchilik 168 foizga oshgan. Yaponiyada 2021-yil may oyida o'sha yilning o'tgan oylariga nisbatan kiberhujumlar 40 foizga oshgan. 2021 yilda ma'lumotlar buzilishi tufayli har soatda o'rtacha 787 671 dollar yo'qotilgan.

2.12-rasm. Global Kiberjinoyatlar statistikasi

2023-yil yanvar oyida Milliy kiberxavfsizlik indeksida (NCI) birinchi o'rinda Gretsiya 96,10 ball bilan qayd etilgan.



2.13-rasm. NCI bo'yicha 5 ta eng yuqori ballga ega mamlakatlar



2.14-rasm. 2021 yilda qit'alar bo'yicha tashkilotlarga qarshi hujumlar

Kiberjinoynatni Mashinani o'rganish usullaridan foydalangan holda aniqlash va statistikasini yaratish. Kiberjinoynat ma'lumotlarini tasniflash uchun qo'llab-quvvatlovchi vektor mashinasi (SVM) va K-yaqin qo'shni (KNN) modellari kabi nazorat ostida tasniflash usullari qo'llaniladi. Xuddi shunday, nazoratsiz tasniflash usuli K-o'rtacha klasterlash, Gauss aralashmasi modeli va noaniq C-vositalari klasterlash va loyqa klasterlash orqali kvazi-tasodifiy klaster usullarini o'z ichiga oladi. Sintetik identifikatsiyani o'g'irlashni aniqlash uchun neyron tarmoqlar qo'llaniladi. Klasterlarni shakllantirish ushbu klasterlash usullaridan foydalangan holda amalga oshiriladi, bu umumiy ma'lumotlardan jinoyat ma'lumotlarini oladi. Kiberjinoynatlarni aniqlashda

CBS StatLine ochiq ma'lumotlaridan olingan ma'lumotlar to'plamidan foydalaniladi. Foydalanilgan atributlar jami foydalanuvchi identifikatori 1000 ga teng bo'lgan shaxsiy xususiyatlar orqali jinoyat qurbonlariga tegishli. Ishlash samaradorligini tahlil qilish uchun turli xil o'quv va sinov ma'lumotlari o'zgaradi. Oxir-oqibat, eng yaxshi texnikadan foydalangan holda, jinoyatchi aniqlanadi va nazoratsiz usulda Gauss aralashmasi modeli aniqlash usuli yordamida yaxshilangan ishlashni ochib beradi. Jinoyatchini aniqlashda 76,56 foiz aniqlikka erishildi. SVM klassifikatori orqali tasniflashda erishilgan aniqlik nazorat qilinadigan usulda 89% ni tashkil qiladi. Turli xil ta'lim va sinov ma'lumotlari o'zgarishi mumkin. Oxir-oqibat, eng yaxshi texnikadan foydalangan holda, jinoyatchi aniqlanadi va nazoratsiz usulda Gauss aralashmasi modeli aniqlash usuli yordamida yaxshilangan ishlashni ochib beradi.

Kiberjinoyat tahlili.

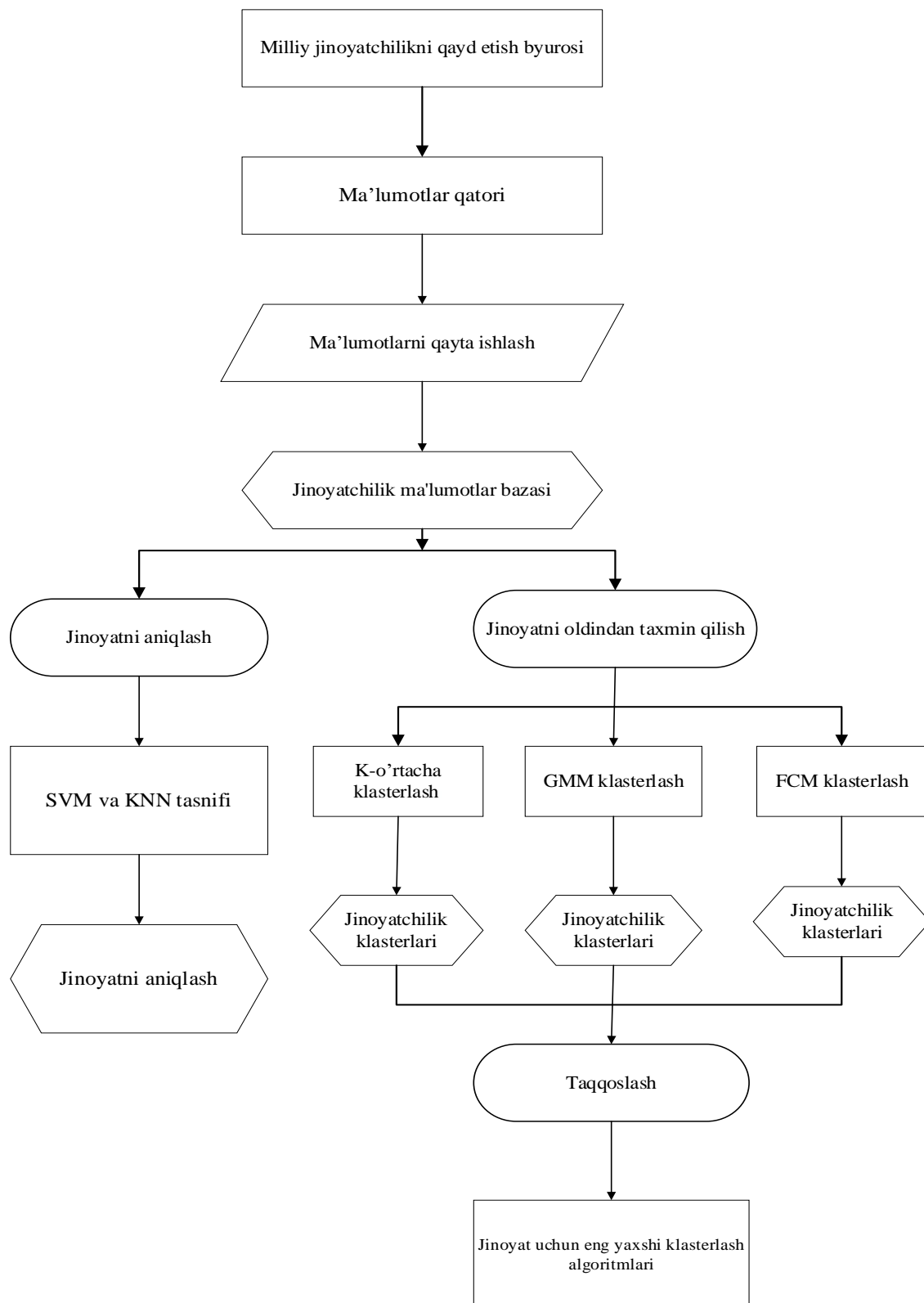
Ma'lumotlar yig'ish. Mas'ul shaxslar hujjatlarida jinoyatlar to'g'risidagi ko'plab ma'lumotlar to'plami mavjud. Har yili butun mamlakat bo'ylab jinoyatlar to'g'risidagi ma'lumotlar holatlar shaklida qayd etiladi va Milliy Jinoyatni qayd etish byurosi bunday yozuvlarning mavjudligini saqlaydi. Odatda, to'plangan ma'lumotlar qayta ishlanmagan va noto'g'ri yoki yetishmayotgan qiymatlarga ega. Ushbu ma'lumotlarni to'g'rilash va ularni to'g'ri shaklga keltirish uchun ma'lumotlarni oldindan qayta ishlash juda muhimdir. Bu ma'lumotlarni tozalash va qayta ishlash jarayonini o'z ichiga oladi.

Tasniflash. Ma'lumotlar to'plami ma'lumotlar ob'yektining ayrim o'ziga xos atributlariga qarab bir necha guruhlarga bo'linadi. Shtat va shaharlarga qarab jinoyatni guruhlash mumkin. Tasniflash jarayoni jinoyatni turli jinoyat turlariga qarab tasniflashni o'z ichiga oladi. K-o'rtacha algoritmidan foydalanib, o'xshash atributlarga ega bo'lgan ma'lumotlarni guruhlash yoki klasterlash mumkin.

Shaklni aniqlash. Bu jarayon jinoyatga tegishli tendentsiyalar va naqshlarni aniqlashni o'z ichiga oladi. Shaklni aniqlashning natijasi ma'lum bir joyga tegishli jinoyat namunasidir. Joylashuvga qarab ob-havo sharoiti, muhim voqea, hududning sezgirligi va jinoiy guruhlarning mavjudligi kabi tegishli atributlar hisobga olinadi. Naqshlar bilan bog'liq bunday ma'lumotlar mas'ul shaxslar xodimlarining muammosiz va samarali ishlashiga yordam beradi.

Bashorat. Tegishli joy uchun model qurilgan. Jinoyat sodir bo'lishi mumkin bo'lgan hududlarni olish uchun joriy sana va atributlar bashorat qilish dasturiga kiritilgan. Vizualizatsiya yordamida natijalar tasvirlanadi.

Vizualizatsiya. Faoliyat darajasini bildiruvchi issiqlik xaritasi orqali jinoyatga moyil hududlarning grafik tasviri mavjud. To'q ranglar past faollikni tasvirlaydi, yuqori faollik esa yorqin ranglar yordamida tasvirlangan.



2.15-rasm. Jinoyatlarni tahlil qilishning turli bosqichlari

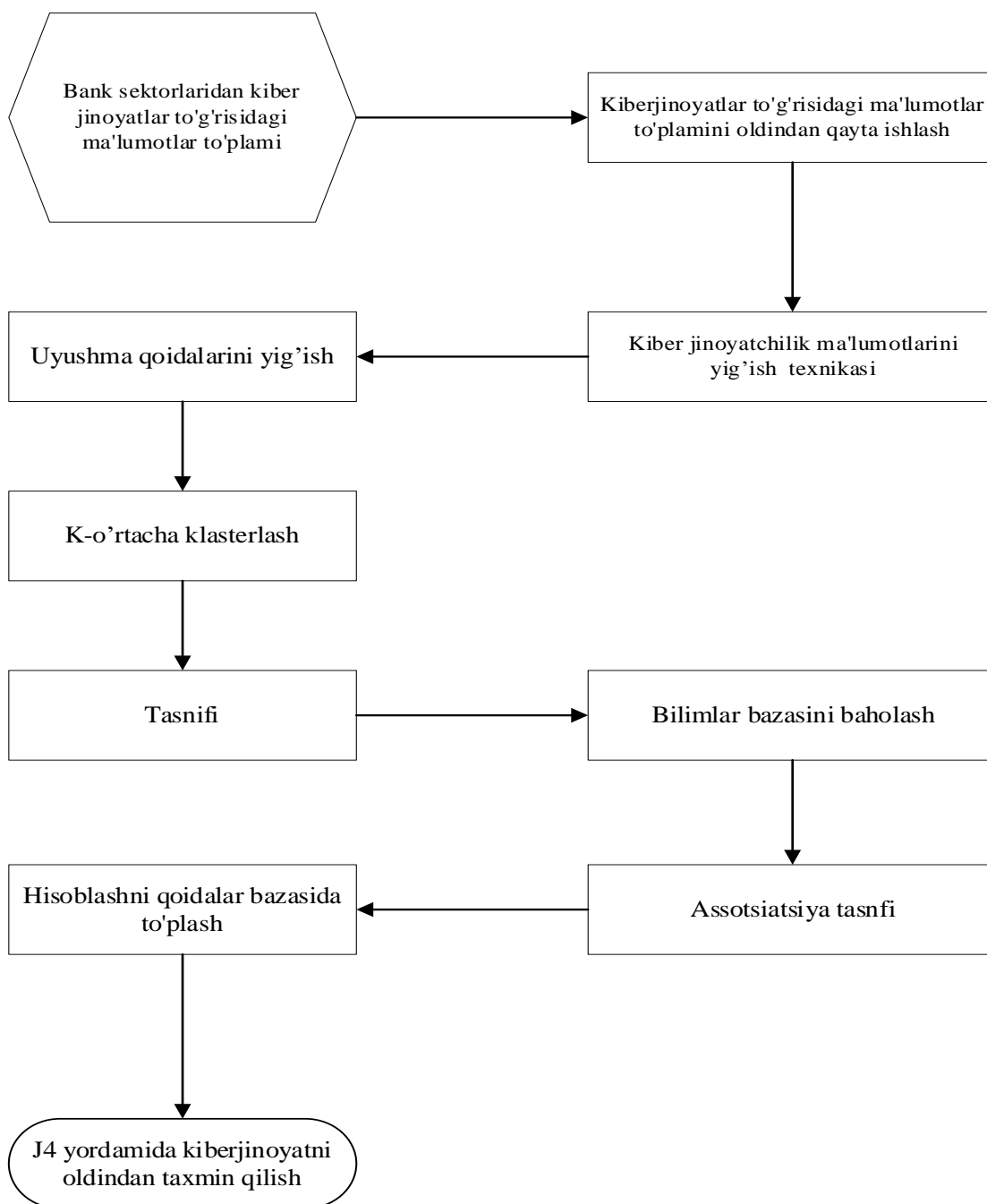
Xakerlar odatda kam rivojlangan davlatlarni nishonga olishadi: qit'a miqyosida Afrika va Osiyoda buzilgan elektron pochta manzillari eng past ko'rsatkichlarga ega. Eng yuqori qoidabuzarliklar Shimoliy Amerikada bo'lib, u yerda 2021-yilda har 2 internet foydalanuvchisidan 1 nafari buzilish sodir bo'lgan. Bu ko'rsatkich jahon o'rtacha ko'rsatkichidan uch baravar yuqori.

Bank sektorida Kiberjinoatlarni aniqlash va statistika yaratish uchun ma'lumotlarni qidirish usullari. Kiberjinoatlarni aniqlash va tadqiq qilish va ularning virtual jinoyatchilarga aloqadorligini tekshirish. Kiberjinoatlar rivojlanishini baholashda ishtirok etadi. Taklif etilayotgan ish K-o'rtacha klasterlash texnikasi, Assotsiatsiya klassifikatori va J48 klassifikatori yordamida Kiberjinoatlarni bashorat qilish modelini taqdim etadi. Bank sektorlarida kiberjinoatlarni bashorat qilish uchun taklif qilingan model kengaytirilgan bashorat natijasini beradi. Shuningdek, u jinoyat ma'lumotlar bazasidan Assotsiatsiya qoidasini yig'ish uchun ta'sirlangan qo'llab-quvvatlash va ishonch tuzilmasidan foydalanadi.

A. Kiberjinoatlar to'plami. Jinoyat namunasini tahlil qilish orqali bank sektoridagi kiberjinoatlar sinfini bashorat qilish uchun turli xil kiberjinoatlar ma'lumotlarini to'plash kerak. Shunday qilib, bu ma'lumotlarni turli xil yangiliklar lentalaridan, maqolalar va bloglardan, internet orqali mas'ul shaxslar bo'limi veb-saytlaridan to'plash kerak. Yig'ilgan kiberjinoatlar ma'lumotlarni qayta ishlash uchun jinoyatlar ma'lumotlar bazasida saqlanadi.

B. Kiberjinoatlar to'plamini oldindan qayta ishlash. Jinoyat ma'lumotlar bazasida saqlangan kiberjinoatlar to'plami ularda ma'lumotlarni qidirish usullarini qo'llashdan oldin, oldindan qayta ishlanishi kerak. Chunki oldindan ishlov berish shovqinli ma'lumotlarni, yetishmayotgan qiymatlarni va hokazolarni olib tashlaydi.

C. Ma'lumotlarni yig'ib olish texnikasi. Oldindan qayta ishlangan ma'lumotlar uchun ma'lumotni yig'ib olish texnikasi va algoritmlari g'ayritabiiy naqshlardan bilim innovatsiyasi orqali firibgarlikni aniqlash yoki prognoz qilish uchun amalga oshiriladi, shuningdek, kredit kartalari bo'yicha kiber firibgarlikka qarshi kurashda e'tirofga erishadi. Jinoyat ma'lumotlar bazalarida to'plangan biznes ma'lumotlarida ko'rinmaydigan aloqalar va havolalar.



2.16-rasm. Kiberjinoyatlarni statistikasini yaratish uchun taklif qilingan model

Klasterlash. Yozuvlar yoki elementlar to'plamini bir nechta guruhlarga bo'lish klasterlash deb ataladi. Klasterlash kiberjinoyat va o'tgan sirli umumiy xususiyatlarga ega bo'lgan jinoiy xususiyatlarni bog'laydigan o'zaro ta'sirlarni aniqlashni nazarda tutadi. Bank sektoridagi firibgarliklarni aniqlash uchun klasterlash usullari qo'llaniladi. Klasterlash nazoratsiz ta'lim sifatida ifodalanadi, chunki uning sinflari aniq emas va aniqlanmagan va ma'lumotlar konsorsiumi faqat nazoratdan iborat. K - bo'lish algoritmi minimalizm va kamroq hisoblash murakkabligi tufayli kiberjinoyatlar ma'lumotlar to'plamini klasterlashda amalga oshiriladi. Dastlab, ma'lumotlar elementlarining miqdori yig'iladi va "k" klasterlari sifatida aniqlanadi. Ob'yektlarning o'rtacha masofalari o'rtasida o'rtacha qiymat mo'ljallangan. Qayta joylashtirish iterativ

usuli elementlarni bir klasterdan ikkinchisiga o'tkazish orqali bo'limlarni tiklash uchun ishlatiladi. Keyin birlashma sodir bo'lgunga qadar, iteratsiyalar soni amalga oshiriladi.

Tasniflash. Tasniflash - bu atributlar misollarini katta miqyosda tasniflashi mumkin bo'lgan modelni yaratish uchun oldindan tasniflangan misollar to'plamini bajaradigan eng ko'p qo'llaniladigan ma'lumotlarni qazib olish usuli. Tasniflash texnikasi ma'lumotlar nuqtalarini xaritalash orqali bog'liq o'zgaruvchi va mustaqil o'zgaruvchi o'rtasida bog'lanish hosil qiladi. Berilgan ma'lumotlar to'plamida tasniflash har bir ma'lumot hodisasi qaysi guruhda bog'langanligini aniqlash uchun ishlatiladi. Tasniflash noma'lum naqshlarning bir nechta modellarini yaratish va oldingi qarorlar asosida istiqbolni baholash uchun ishlatiladi. Avtomatik kredit avtorizatsiyasi bank sektori va moliya tashkilotlarida deyarli asosiy protsedura hisoblanadi. J48, CART va boshqalar kabi qarorlar daraxtlari asosida tasniflash ko'rinishidan foydalangan holda kredit roziligi uchun yuqori baho yaratish orqali firibgarliklarni taqiqlash mumkin.

Assotsiatsiyalar tasnifi. Aniqroq bo'lish uchun assotsiativ tasniflash juda yangi va takomillashtirilgan usul bo'lib, assotsiatsiya qoidalarini va modelni bashorat qilish tasniflarini o'zlashtiradi. Ushbu usul ob'yektlar to'plamidagi bog'lanish va assotsiatsiyani istisno qilish uchun amalga oshirilmoqda. Assotsiativ tasnif nazoratsiz o'rganish ostida bo'ladi, chunki u qoidalarni chiqarish uchun har qanday sinf xarakteristikasini jalb qiladi.

J48 yordamida Kiberjinoyatlarni statistikasi. Kiberjinoyatlarni bashorat qilish tahlilidagi muammolar va muammolarni tasniflash uchun J48 algoritmi aniqroq va aniqroqdir.

J48 algoritmi daraxtni qurish uchun kesish usulidan foydalanadi. Azizillo texnikasi tegishli ma'lumotlarni olib tashlash orqali daraxt bo'lsa hajmini kamaytiradi. Kutilayotgan J48 algoritmi ma'lumotlarni to'liq toifalashgacha tasniflaydi va kiberjinoyat ma'lumotlarini o'qitishda eng yuqori aniqlikni ta'minlaydi. Bundan tashqari, aniqlik va silliqlikni barqarorlashtiradi. J48 algoritmi daraxti C4.5 ning keng ko'lamli versiyasidir. J48 algoritmi qoidalar to'plami va qarorlar daraxti ko'rinishida tasniflagich chiqishini ishlab chiqaradi. Qoidalar to'plamini tanib olish oson va ilova ichida ishlatish uchun juda oson.

Xulosa

- Kiberjinoyatlar, kompyuter tarmoqlari orqali amalga oshiriladigan hujumlar va zararli faoliyatlar to'plamini ifodalaydi.
- Ushbu hujumlar shaxsiy ma'lumotlarni olish, to'lov sistemalarini xak etish, tarmoq xizmatlarini buzish va boshqa zararli faoliyatlar shakllarida ro'y beradi.
- Kiberjinoyatlar, hukmdorlik, kompaniyalar, sohalarning boshqaruv markazlari, shaxslar va umumiy foydalanuvchilar uchun katta xavf tashkil etadi.
- Kiberjinoyatlar, yuridik va iqtisodiy zararlar, shaxsiy hamjihatlikning buzilishi, axborotni boshqarish va xavfli infrastruktur tuzilishlariga olib keladi.

FOYDALANILGAN ADABIYOTLAR:

- S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O'quv qo'llanma. – T.: «Aloqachi», 2020, 221 bet.
- Cyber Security Policy Guidebook
- Jennifer L. Bayuk Independent Cyber Security Governance Consultant Industry Professor at Stevens Institute of Technology, Hoboken
- NJ Jason Healey Director of the Cyber Statecraft Initiative Atlantic Council of the United States, Washington
- D.C. Paul Rohmeyer Information Systems Program Director Howe School of Technology Management Stevens Institute of Technology, Hoboken
- NJ Marcus H. Sachs Vice President for National Security Policy Verizon Communications, Washington
- D.C. Jeffrey Schmidt Chief Executive Officer JAS Communications LLC, Chicago, IL
Joseph Weiss Professional Engineer Applied Control Solutions, LLC, Cupertino, CA