S.Y.YUSUPOV,
SH.R.GULOMOV, N.B.NASRULLAYEV

RAQAMLI KRIMINALISTIKA

O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI
VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT
AXBOROT TEXNOLOGIYALARI UNIVERSITETI

S.Y.YUSUPOV,
SH.R.GULOMOV, N.B.NASRULLAYEV

RAQAMLI KRIMINALISTIKA

O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligi tomonidan o‘quv qo‘llanma sifatida tavsiya etilgan.

TOSHKENT – 2020

UDK: 004(075.8)
KBK: 32.973я722
Y-91

S.Y.Yusupov, Sh.R.Gulomov, N.B.Nasrullayev. Raqamli kriminalistika: o'quv qo'llanma. – T.: «Aloqachi», 2020, 240 bet.

ISBN 978–9943–6394–0–9

O'quv qo'llanma raqamli kriminalistikaning asosiy tushunchalari, vazifalari va ko'rinishlari, kompyuter jinoyatlarini tadqiq qilish va ekspert faoliyatida kompyuter texnologiyalari va kompyuter texnikalarini nazariy va amaliy asoslarini qo'llanilishi ifodalagan «Raqamli kriminalistika» nomi ostidagi fanning bo'limiga bag'ishlangan.

O'quv qo'llanma «Axborot xavfsizligi» va «Kriptologiya va kriptoanaliz» ixtisosligi bo'yicha ta'lim olayotgan magistratura talabalari uchun mo'ljallangan bo'lib, faoliyati axborot xavfsizligini ta'minlash va kompyuter jinoyatlarini tadqiq qilish bilan bog'liq bo'lgan mutaxassislarning keng doirasi uchun ham foydali bo'lishi mumkin.

UDK: 004(075.8)
KBK: 32.973я722

Taqrizchilar:

Sevinov J.U. – texnika fanlari doktori, Islom Karimov nomidagi Toshkent davlat texnika universiteti «Axborotlarga ishlov berish va boshqarish tizimlari» kafedrasi mudiri.

Musayev M.M. – texnika fanlari doktori, Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti «Kompyuter tizimlari» kafedrasi professori.

Mas'ul muharrir:
A.A.Ganiyev.

ISBN 978–9943–6394–0–9

KIRISH

Oxirgi yigirma yillikda butun dunyoda kompyuter texnikasi va yangi axborot texnologiyalaridan foydalangan holda sodir etiladigan jinoyatlarning keng miqyosdagi o‘sishi kuzatilmoqda. Kompyuter texnikasidan foydalangan holda sodir etiladigan jinoyatlar yuqori darajadagi latentlik va past darajadagi fosh etilish bilan xarakterlanadi, va bu “kompyuter jinoyatchiligi”ni juda foydali va yetarlicha xavfsiz ish sifatida ko‘rsatadi. Qayd qilingan kompyuter jinoyatlari va kompyuter bezoriliklarining sezilarli darajadagi zararlari sonining o‘sishi kuzatilmoqda. Oddiy bank o‘g‘riligida bir martada bir necha o‘n ming dollar atrofida olib ketiladi, vaholanki o‘rtacha bank axborot tizimiga kompyuter orqali buzib kirilishi bugungi kunda millionlab dollar zarar keltirmoqda.

Kompyuterlar, kompyuter tarmoqlari, raqamli texnikalar noqonuniy harakatlar obyekti bo‘lib bormoqda:

- noqonuniy buzib kirishlar, xakerlik hujumlari;
- ma’lumotlar bazasini modifikatsiyasi, buzilishi yoki yo‘q qilinishi;
- axborotni o‘g‘irlanishi yoki nusxalanishi;
- pul mablag‘larini o‘g‘irlanishi, to‘lov vositalari firibgarligi (bank-mijoz va boshqalar);
- viruslar va boshqa zararkunanda dasturiy ta’minotlardan foydalanish;
- shaxsiy kompyuterlardan hujumlarni va boshqa zararli harakatlarni boshqa shaxsiy kompyuterlar va lokal tarmoqlarda uyushtirish uchun foydalanish;

Bu jinoyatlarni tergov qilish bilan fanning “Raqamli kriminalistika” yoki ingliz tilida “Forenzika” deb nomlanuvchi bo‘limi shug‘ullanadi.

Respublikamizda axborot texnologiyalarining rivojlanishi bilan bir qatorda xo‘jalik va davlat boshqaruvi organlarida raqamli kriminalistikaning vazifalari va predmeti, kriminalistikani tadqiq qilish vositalari va usullari hamda kompyuter jinoyatlarini sodir etish yo‘llariga alohida e’tibor qaratilmoqda. Shu sababli ma’lumotlarni qayta tiklash, ma’lumotlarni va ma’lumot tashuvchilarni kompyuter ekspertizasi bo‘yicha sezilarli natijalarga erishildi hamda axborot xavfsizligi insidentlariga qarshi reaksiya rejasi va tergov bosqichlarini yaratish boshlandi. Shu bilan birga raqamli steganografiya vositalari va usullari va axborotni kiberjinoyatdan himoyalash yo‘llarini

takomillashtirish talab etiladi. O‘zbekiston Respublikasi Prezidenti Sh.M.Mirziyoyevning 2017 yil 8 fevraldagi “Qonun hujjatlarini tarqatish tizimini tubdan takomillashtirish chora-tadbirlari to‘g‘risida”gi qarorida va 2017-2021 yillarda O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasida vazifalar belgilab olindi, shular qatorida «...axborot xavfsizligini ta’minlash va axborotni himoya qilish tizimini takomillashtirish, axborot sohasidagi tahdidlarga o‘z vaqtida va munosib qarshilik ko‘rsatish» va kiber jinoyatchilikni fosh etish masalalariga alohida e’tibor qaratilgan. Bu vazifalarni amalga oshirish eng muhim muammolardan biri hisoblanadi.

Mazkur o‘quv qo‘llanma kompyuter jinoyatlarini tadqiq qilish va ekspert faoliyatlarida kompyuter texnologiyalari va kompyuter texnikasini qo‘llashning nazariy va amaliy asoslarini o‘z ichiga oladi.

Qo‘llanmaning birinchi bobida raqamli kriminalistikaning vazifalari, ko‘rinishlari va asosiy tushunchalari, uning qo‘llanilish sohasi, kriminalistikani tadqiq qilish usullari hamda qidiruv usullari, raqamli dalillarni aniqlash va ta’minlashga qarshilik qilish – kontr-forenzika masalalari ko‘rib chiqilgan. Maxsus texnik vositalar, kriminalistik fototasvirlar va videoyozuvlar hamda kriminalistik axborot tizimlaridan iborat raqamli kriminalistika vositalari keltirilgan.

Ikkinchi bobda kompyuter jinoyatlarining asosiy yo‘nalishlari, kompyuterlar ishlariga aralashishlar va kompyuterlardan kerakli texnik vosita sifatida foydalanish bilan bog‘liq ularning toifalari, Interpolning Bosh Sekretariati kodifikatori bo‘yicha kompyuter jinoyatlarining klassifikatsiyasi, kompyuter jinoyatchilarining ko‘rinishlari ko‘rib chiqilgan. Kompyuter jinoyatlarini sodir etish yo‘llari va kompyuter jinoyatlarini turli ko‘rinishlari keltirilgan.

Qo‘llanmaning uchinchi bobida kompyuter jinoyatlarini ogohlantirish choralarining asosiy guruhlari keltirilgan, kompyuter jinoyatlarining katta qismi tashkilot va korxonalarda tashkiliy choralarning yetishmovchiligi, ma’lumotlarni ruxsatsiz kirishdan kuchsiz himoyalanganligi, maxfiylikning yetarli emasligi, xodimlarning kuchsiz tekshiruvi va ko‘rsatmasi oqibatida sodir etilishi ko‘rsatilgan. Kompyuter jinoyatlarini ogohlantirish mexanizmlari va ikki tashqi va ichki toifaga ajratilgan jinoyat izlarini tadqiq qilish keltirilgan.

To‘rtinchi bob insidentlarni boshqarishdagi murakkabliklar, hujum oqibatlari, sabablari va ularning paydo bo‘lish yo‘llarini aniqlanuvchi insidentlarni tadqiq qilish masalalarini ko‘rib chiqishga bag‘ishlangan. Insident toifalari va klassifikatsiyasi hamda axborot xavfsizligi

insidentlarini namunaviy tahlillash tadqiq qilinadi. Klassik steganografiya yo‘nalishi – xabarlarni yashirin yuborish tizimiga qarshi hujumlar toifalari va qo‘shimcha axborotlarni raqamli obyektlarga joriy qilish yoki yashirishga asoslangan raqamli steganografiya ko‘rib chiqilgan.

Beshinchi bobda kompyuter vositalari va tizimlarini kriminalistik tadqiq qilish, ular natijasida olingan axborot, kompyuter-texnik ekspertizalar ko‘rinishlarida dalil sifatida ishlatilishi mumkinligi ko‘rib chiqiladi. Bu yerda ikkita ekspert tizimlari – tez, stabil va erkin foydalanish uchun yaratilgan, sud organining raqamli yechimni yagona izohlovchi va raqamli kriminalistikada foydalaniluvchi sud organi to‘plami instrumentlari (FTK) va ikkinchisi esa ekspertlarga tayyor filtrlar va modullar keng spektri yordamida ma’lumotlarni yozish, axborotni kriminalistik tahlillash yo‘li bilan potensial dalillarni aniqlash va olingan dalillar ishonchliligi va butunliligini saqlagan holda olingan natijalar haqida to‘liq hisobotlarni tayyorlash imkonini beruvchi kompyuter ekzpertizalarining barcha bosqichlarini o‘tkazish uchun (EnCase Forensic) texnologiya va dasturlari.

Oltinchi bob zamonaviy kiber jinoyatchilik muammolariga bag‘ishlangan, kiber jinoyatchilik o‘sishining asosiy sabablari va kiber jinoyatlar hisoblanuvchi faoliyatlar keltirilgan. Kiber jinoyatchilikni ogohlantirish sohasidagi yondashuvlar va usullar, tashkiliy ishlar, tamoyillar ko‘rib chiqilgan.

O‘quv qo‘llanma 5A330302 - «Axborot xavfsizligi» va 5A330301 -«Kriptografiya va kriptoanaliz» mutaxassisligi bo‘yicha ta’lim olayotgan magistratura talabalari uchun tavsiya etiladi, hamda faoliyati axborot xavfsizligini ta’minlash va kompyuter jinoyatlarini tadqiq qilish bilan bog‘liq bo‘lgan mutaxassislarning keng doirasi uchun ham foydali bo‘lishi mumkin.

1. RAQAMLI KRIMINALISTIKA TUSHUNCHASI, VAZIFALARI VA VOSITALARI

1.1. Raqamli kriminalistikaning asosiy tushunchasi

So‘nggi yuz yillikning 70-yillarining oxirlarida yuridik adabiyotlarda barcha kompyuter axboroti, axborot texnologiyalari bilan bog‘liq jinoyatlarning yangi ko‘rinishlari paydo bo‘layotgani haqida fikrlarni aniq bildira boshlashdi. Bunga muvofiq bu ko‘rinishdagi jinoyatlar bilan kurashishga yo‘naltirilgan maxsus usullar va vositalarni qamrab oluvchi kriminalistikaning yangi yo‘nalishi shakllana boshlandi.

Shu bilan birga ushbu sohada jinoiy-huquqiy nazoratlash malakasini yo‘qligi, texnik jihatlarni tushunishdagi qiyinchiliklar va bu ko‘rinishdagi jinoyatlarning o‘ziga xosligi uzoq vaqt kriminalistika bo‘yicha adabiyotlarda bir vaqtning o‘zida bir nechta uning nomlari mavjud bo‘lishiga olib keldi: «axborot jinoyatlari», «kompyuter jinoyati», «yuqori texnologiyalar sohasidagi jinoyat», «kommunikatsion jinoyat», «tarmoq jinoyati», «mashina-intellektual yoki texnik-intellektual jinoyat».

Ushbu hosil bo‘lgan vaziyatga javob variantlaridan biri N.N.Fedotovning sud dalillarini yig‘ish uchun atrof holatni tadqiq qilishning texnologik usullari va ilmiy fanlarni butun sohasini o‘rganuvchi fan - «forensic science» yoki «forensic» so‘zidan hosil bo‘lgan «computer forensic» ingliz termini - «forenzika» tushunchasini kiritish haqidagi taklifi bo‘ldi.

Shunday qilib, ***«Raqamli kriminalistika»*** yoki ***«forenzika»*** termini lotin tilidan olingan «foren» so‘zi bo‘lib, «forum oldidan so‘z», ya’ni sud, sud bahsi oldida chiqish deganidir. Bu fan kompyuter jinoyatlarini aniqlash va fosh etish, foydalanilayotgan vositalar haqida tizimli uzilishlarni tadqiq qilish va axborotni yig‘ish dalillarini olish yo‘llari haqidadir.

Raqamli kriminalistika (digital forensics) – kompyuterlar, ma’lumotlarni saqlash tizimlari, kompyuter tarmoqlarida, mobil va boshqa raqamli qurilmalarda joylashgan raqamli dalillarni yig‘ish va jinoyatlarni (insidentlarni) tadqiq qilish haqidagi amaliy fan, kriminalistikaning bir bo‘limi.

Raqamli kriminalistika masalalari bu raqamli dalillarni saqlash, identifikatsiya qilish, olish va hujjatlashtirish hisoblanadi.

Raqamli jinoyat:

– raqamli texnikaga qarshi yo‘naltirilgan jinoyat;

– raqamli texnika dalillarni saqlab qoluvchi jinoyat;

– raqamli texnika yordamida amalga oshiriluvchi jinoyat.

Forenzikaning qo‘llanilish sohasi: kompyuter axboroti tajovuz obyekti, kompyuter esa jinoyatni sodir etish quroli, hamda qandaydir raqamli dalillar kabi shakllanuvchi hodisalarni tadqiq qilish. Avvaliga kompyuter jinoyatlari uch yo‘nalishi ajratilgan:

– kompyuterni, hisoblash tizimini yoki kompyuter tarmog‘ini pul, mulk yoki xizmatlarni olish maqsadida foydalanish yoki foydalanishga urinish;

– kompyuter, hisoblash texnikasi, kompyuter tarmoqlari yoki ulardagi matematik ta’minot, dasturlar yoki axborotni o‘zgartirish, zarar yetkazish, yo‘q qilish yoki o‘g‘irlash maqsadida qasddan qilingan ruxsatsiz harakat;

– kompyuterlar, hisoblash tizimlari yoki kompyuter tarmoqlari orasidagi aloqalarni qasddan ruxsatsiz buzish.

So‘nggi yillarda insidentlar soni geometrik progressiya bo‘yicha oshmoqda, quyidagi terminlar almashdi: «axborot jinoyati», «axborot texnologiyalaridan foydalangan holda sodir etilgan jinoyat», «kiberjinoyat» va hozirda kompyuter jinoyatlarini uch yo‘nalishga ajratiladi:

– axborot xavfsizligiga qarshi jinoyat;

– elektron axborot boshqa jinoyatni sodir etish vositasi sifatida hisoblanuvchi jinoyat;

– kompyuter va boshqa elektron texnikadan foydalangan holda sodir etiladigan jinoyat.

Kompyuter jinoyati milliy va iqtisodiy xavfsizlikka jiddiy tahdid soladi va 70-yillardan boshlab ilg‘or davlatlarda kompyuter jinoyatlari bilan kurashish bo‘yicha maxsus bo‘limlar yaratilmoqda, oliy ta’lim muassasalarida axborot jinoyatlarini tadqiq qilish usuli bo‘yicha kurslar o‘qilmoqda.

Bu kurslar kompyuter jinoyatchiligi bilan kurashishning quyidagi asosiy yo‘nalishlarini qamrab oladi:

1. Insidentlarga reaksiya qilish (Incident response)
2. Insidentlarni tergov qilish (eDiscovery)
3. Raqamli kriminalistika (Digital Forensic)
4. Insidentlar monitoringi (Monitoring Incidents).

Raqamli kriminalistika kompyuter jinoyatlarini tergov qilishning asosiy yo‘nalishlaridan biri hisoblanadi. Mutaxassis-kriminalistlar o‘z

ishlari davomida ularga insident sababini va xronologiyasini o‘rnatish, hujumni amalga oshirish maqsadlari va usullarini aniqlashtirish hamda aloqador shaxslarni ko‘rsatish imkonini beruvchi maksimal ma’lumotlarni tahlil qiladi.

Raqamli axborotni tashuvchilarni tahlillash vaqtida mutaxassislar hodisalar xronologiyasini qayta tiklashadi; fayl tizimlari, operatsion tizimlar, ilovalar jurnallarini tahlillaydi; operatsion tizim reyestri kalitlarini o‘rganishadi; zararkunanda dasturiy ta’minot yo‘qligiga tashuvchini tadqiq qilishadi. Yana kompyuter kriminalistika doirasida maxsus yo‘nalishni - funksional, zararkunanda dasturlar ishining algoritmi va tarmoq aloqalarini o‘rganishga yo‘naltirilgan virusli analitikani ham ta’kidlash lozim.

Raqamli kriminalistikani qo‘llash sohalari:

1. Kompyuter axboroti tajovuz obyekti, kompyuter esa jinoyatni sodir etish quroli, hamda qandaydir raqamli dalillar kabi shakllanuvchi jinoyatlarni tadqiq qilish va fosh etish.

2. Dalillar kompyuter axboroti ko‘rinishiga ega bo‘lganda fuqarolik ishlari uchun dalillarni yig‘ish va tadqiq qilish. Ayniqsa bu huquqlar obyekti kompyuter axboroti ko‘rinishida – EHM uchun dastur, raqamli shaklda, Internet tarmog‘idagi tovar belgisi, domen nomi va shu kabilar tarzida ko‘rsatilganda ayniqsa intellektual mulk huquqlarini buzilishi haqidagi ishlar bo‘yicha dolzarbdir.

3. Sug‘urta obyekti kompyuter axboroti ko‘rinishida ko‘rsatilgan yoki bunday obyekt bo‘lib axborot tizimi hisoblanganda sug‘urta firibgarligi, shartnoma shartlarini buzilishiga tegishli sug‘urta kompaniyalari tomonidan o‘tkaziladigan sug‘urta tadqiq qilish ishlari.

4. Axborot tizimlariga tegishli xavfsizlik insidentlarini korxona ichki tadqiq qilish ishlari, hamda tijoriy sir va boshqa maxfiy ma’lumotlardan iborat axborotni chiqib ketishini oldini olish bo‘yicha ishlar.

5. Dushman axborot tizimi va shaxsiy tizim himoyasiga ta’sir o‘tkazish jarayonida kompyuter axborotini izlash, yo‘q qilish va qayta tiklash bo‘yicha harbiy va razvedka vazifalari.

6. Fuqarolarning elektron ko‘rinishdagi shaxsiy axborotini himoyasi bo‘yicha vazifalar, bu elektron hujjatlar va axborot tizimlari bilag bog‘liq bo‘lganda o‘z huquqlarini himoyalash.

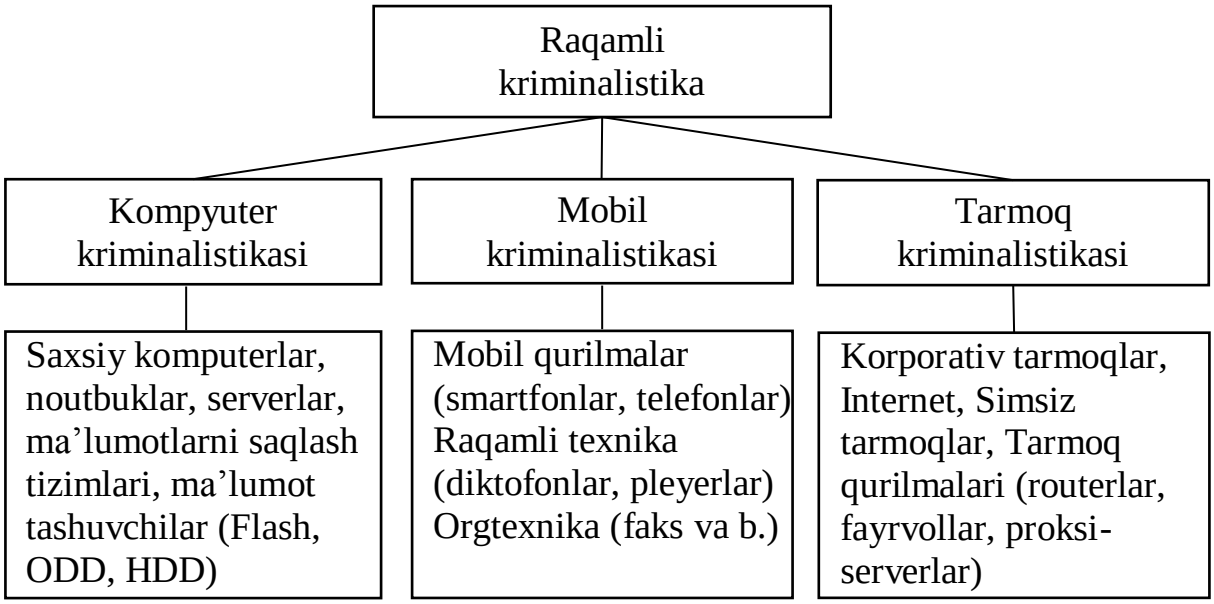
Ko‘plab bu ilovalarda forenzikaning ba’zi usullari axborotni texnik himoyasi usullari bilan juda mustahkam integratsiyalangan.

Shunday qilib, **«Raqamli kriminalistika»** yoki **«Forenzika»** kompyuter axboroti bilan bog‘liq jinoyatlarni tadqiq qilish va fosh etish haqidagi, kompyuter axboroti shakliga ega dalillarni tadqiq qilish va olish usullari haqidagi, bu uchun qo‘llaniladigan texnik vositalar haqidagi amaliy fan hisoblanadi.

1.2. Raqamli kriminalistikaning turlari

Raqamli kriminalistikani uch turga ajratish mumkin (1-rasm):

«Kompyuter kriminalistikasi» - bu ilm va san’at, u qayta tiklash uchun maxsus usullardan foydalanishni, kompyuter jinoyatlari bilan bog‘liq elektron ma’lumotlar tahlili va haqiqiyligini tekshirishni talab etadi. Unda qonun bilan kompyuter ilmlari, axborot texnologiyalari va boshqa texnik masalalar birlashtiriladi.



1- rasm. Raqamli kriminalistikaning turlari

«Tarmoq kriminalistikasi» - ancha oldin paydo bo‘lgan va xavfsizlik tahlili bo‘yicha mutaxassislar ancha yillardan beri Wireshark va boshqa trafik analizatorlaridan foydalanishadi. Birinchidan, foydalanuvchilar maksimal tezroq shubhali harakatlarni aniqlash maqsadida tarmoq kriminalistikasi vositalariga faolroq tayanadigan bo‘lishdi. Ikkinchidan, xavfsizlik tizimlari ishlab chiquvchilar bunday shubhali harakatlarni aniqlash bo‘yicha ixtisoslashgan yechimlar yaratishdi.

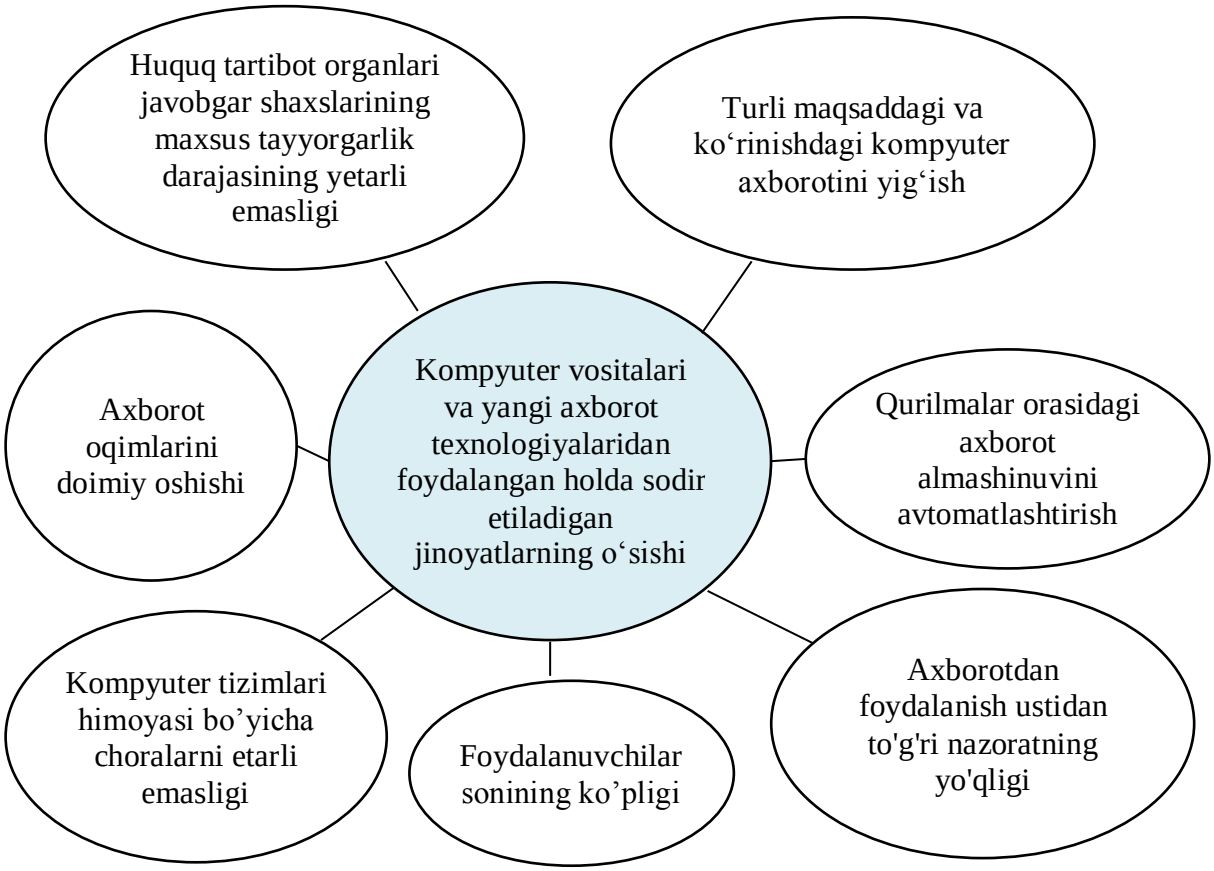
«Mobil kriminalistika» - uyali aloqa mavzulariga qo‘llaniluvchi – mobil qurilmalarning raqamli ma’lumotlarini olish va dekodlash imkoniyati.

Kompyuter vositalari va yangi axborot texnologiyalaridan foydalangan holda sodir etiladigan jinoyatlarning o‘sishi 2-rasmda keltirilgan faktorlar bilan tushuntiriladi. Kompyuter texnika vositalari va yangi axborot texnologiyalaridan foydalangan holda sodir etiladigan jinoyatlarning turi va soni doimiy o‘smoqda. Bunday jinoyatlarni sodir etishda tajovuz qilish predmetlarini ikki guruhga ajratish mumkin:

– kompyuter texnikasining o‘zi va axborot;

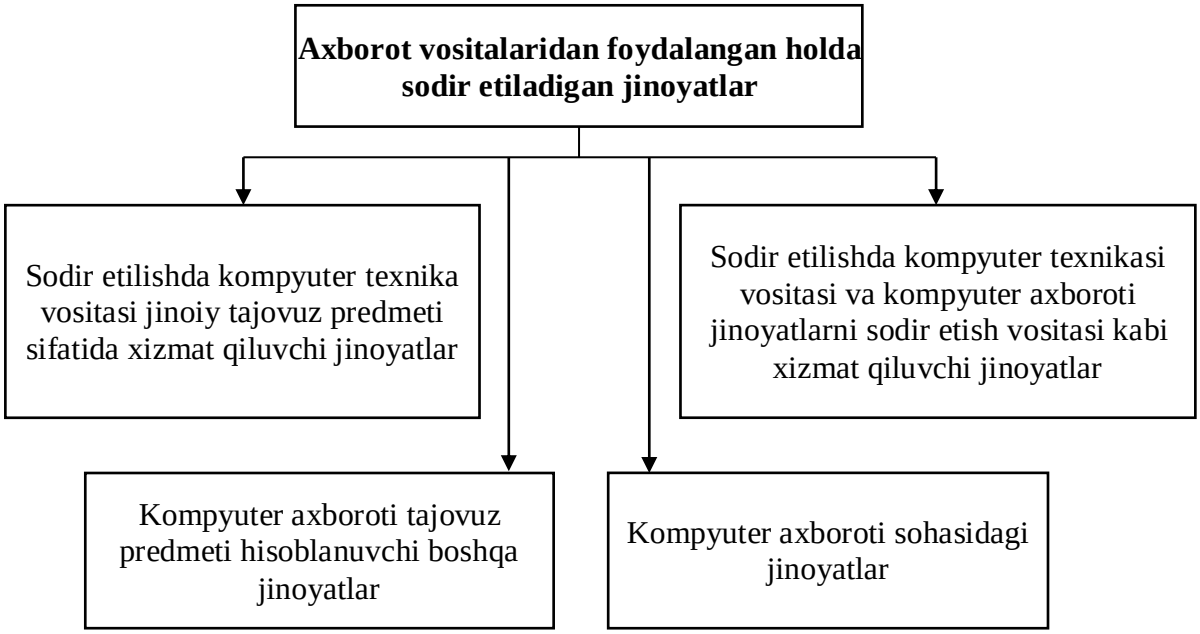
– kompyuter texnikasi va axborotdan jinoiy tajovuz qilish quroli kabi foydalanilib hujum qilinilishi mumkin bo‘lgan obyektlar.

Axborot vositalarining qo‘llanilishi bilan sodir etiladigan barcha jinoyatlarni mos holda to‘rt guruhga ajratish mumkin (3-rasm):



2- rasm. Kompyuter vositalaridan foydalangan holda sodir etiladigan jinoyatlarning o‘sish tuzilmasi

Mulkka qarshi jinoyatni sodir etishda – o‘g‘irlash, yo‘q qilish, zarar yetkazishda jinoiy tajovuz predmeti sifatida kompyuter texnikasi xizmat qiladi. Tajovuz qilish predmeti sifatida texnik vositalarning o‘zi moddiy ob’ekt kabi xizmat qiladi. Kompyuter texnikasi va axborot jinoyat sodir etish vositasi sifatida ham xizmat qilishi mumkin. Bu ma’noda kompyuter qurol yoki transport vositasi sifatida jinoyat quroli kabi bir qatorda ko‘rilishi mumkin.



3- rasm. Axborot vositasidan foydalangan holda sodir etiladigan jinoyatlar sxemasi

Sodir etishda qurol sifatida kompyuter texnikasi va axborot qo‘llaniladigan keng tarqalgan jinoyatlarga turli qurilmaviy-dasturiy vositalardan (masalan, zararkunanda dasturlar) foydalanilib mulkning bu ko‘rinishiga avtomatlashtirilgan ma’lumotlar bankiga o‘zgartirishlar kiritish yo‘li bilan moddiy vositalarni o‘g‘irlash, ikkinchidan moddiy axborot tashuvchilarni o‘g‘irlanishi bilan bog‘liq jinoyatlar kiradi.

1.3. Raqamli kriminalistikaning vazifa va predmetlari

Raqamli kriminalistika texnik, huquqiy xarakterdagi va kadrlarni tayyorlash sohasida quyidagi muammolarga ega:

1. Texnik:

– raqamli tashuvchilardan ma’lumotlarni olish;
– axborotni qayta tiklash;

– ma’lumotlarni izlash, tahlillash va intrepretatsiyalash;
– raqamli dalillarni saqlanuvchanligini ta’minlash.

2. Huquqiy:

– yig‘ilgan ma’lumotlarni isbotlanuvchanligi;
– meyoriy baza.

3. Mutaxassislar tayyorgarligi:

– raqamli tizimlar ishining fizik tamoyillarini va kompyuter kriminalistikasi vositalarini bilish;
– texnik va huquqiy tomonlarini bilish.

Ma’lumotlarni olish:

1. Ruxsat etilmagan ma’lumotlarni nusxalash (ma’lumotlarni tasodifiy va atayin modifikatsiyalash imkoniyati).
2. Nusxani originalga mos kelishi (xeshlash, xesh-funksiya tanlovi).
3. Nusxaning to‘liqligi (buzilgan ma’lumotlarning «yashirin» va zahira sohasi).
4. Nusxalash tezligi (ma’lumot yig‘uvchilarni katta hajmi).
5. Nusxaning saqlanganligi. Ish jarayonida ishlash, transportirovka, nusxalarni saqlash.
6. Ma’lumotlarni himoyalash, axborotni chiqib ketishini oldini olish.

Ma’lumotlarni qayta tiklash:

1. Buzilgan ma’lumotlarni qayta tiklash.
– apparat va dasturiy xatolar;
– zararkunanda DT ta’siri;
– foydalanuvchilarning xatoligi va atayin harakatlari.
2. «Yopiq» ma’lumotlarni qayta tiklash.
– parol bilan yopilgan ma’lumotlar;
– kodlashtirilgan va shifrlangan ma’lumotlar;
– «yashirin» sohalardagi ma’lumotlar.
3. Ma’lumotlarni saqlash tizimidan qayta tiklash.
– RAID tizimlari va tashqi DAS tizimlari;
– NAS tarmoq ombori;
– ma’lumotlarni virtual va taqsimlangan ombori.
4. Ma’lumotlarni saqlashning turli texnologiyalari.
– ma’lumot saqlovchilarni toifalari;
– interfeyslar;
– ma’lumotlar saqlashni tashkillashtirish yo‘llari.

Bu muammolarga muvofiq raqamli kriminalistika quyidagi vazifalarni yechadi:

– kompyuter axboroti bilan bog‘liq harakatlar va tezkor-qidiruv tadbirlari (TQT) taktikasini ishlab chiqish;

– kompyuter jinoyati dalillarini tadqiq qilish va yig‘ish uchun apparat va dasturiy vositalar, usullarni yaratish;

– kompyuter axboroti bilan bog‘liq huquqbuzarliklarning kriminalistik xarakteristikasini o‘rnatish.

Forenzika bo‘yicha mutaxassis ishlashiga to‘g‘ri keladigan deyarli barcha izlar doimiy yoki salbiy kompyuter axboroti ko‘rinishiga ega. Ularni yo‘q qilish etarlicha oson – ham qasddan, ham tasodifan. Ularni qalbakilashtirish oson, «qalbaki» bayt «haqiqiysidan» farqlanmaydi.

Raqamli dalillarni qalbakilashtirilishi axborotni mazmuni bo‘yicha yoki boshqa joylarda qoldirilgan axborot izlari bo‘yicha aniqlanadi. Raqamli dalillarni bevosita inson sezgi organlari orqali qabul qilish mumkin emas, biroq faqatgina murakkab qurilmaviy-dasturiy vositalar orqaligina qabul qilish mumkin. Shuning uchun ham bu izlarni boshqa shaxslarga – prokurorlarga, sudyalarga tushunarli qilib ko‘rsatish qiyin. Har doim ham ularni saqlashda izlarni o‘zgarmasligini ta’minlash oson emas. Nafaqat ta’minlash, balki sudyaga buni o‘zgarmasligini isbotlash ham. Umuman, «o‘zgarmaslik» tushunchasi kompyuter axborotiga tor holatdagina qo‘llaniladi. Ba’zi bir ma’lumot tashuvchilarda ular rostdan ham statik – tashuvchi sohalarini turli magnitlanishi ko‘rinishida yoki uning optik xususiyatlarini turi ko‘rinishida saqlanadi. Biroq boshqa holatlarda axborotni saqlash usullari shundayki, ma’lumot tashuvchini doimiy almashinuvini ko‘zda tutadi.

Kompyuterning tezkor xotirasi bir necha millisoniyada regeneratsiyalanadi. Ya’ni u yerda yozilgan signallar o‘chiriladi va yana qayta yoziladi. Ko‘plab aloqa kanallari bo‘yicha yuborishda yuzaga keluvchi xatoliklar hisobida xalaqitga bardoshli kodlashtirishdan foydalaniladi; bu xatoliklar paydo bo‘lishidan qochib bo‘lmaydi, biroq kod ortiqchaligi hisobiga qabul qiluvchi tomonidan tuzatiladi. Markaziy protsessorda ham doimiy ravishda arifmetik-mantiqiy operatsiyalarni bajarishda xatoliklar bo‘ladi, biroq ular juda ham ko‘p bo‘lmasa ichki diagnostika sababli tuzatiladi. TCP (Transmission Control Protocol, yuborishni boshqarish protokoli) kabi tarmoq protokollarida bu ishonchlilik yo‘lda yo‘qolgan datagrammalar yoki boshqa axborot bloklari ularning to‘g‘ri qabuli tasdiqlanmaguncha oldindan yuborilishi hisobiga erishilgan.

Raqamli kriminalistikaning **predmetlari** quyidagilar:

– Axborot texnologiyalari – ham jinoyatlarni oldini olish uchun, ham ularni sodir etish uchun foydalanish imkoniyati.

– Amaliy dasturiy ta’minotni o‘rganish usullari.

– Kriminal amaliyot – jinoyatlarni sodir etish yo‘llari va qurollari, ularning oqibatlari, qoldiradigan izlari, jinoyatchining shaxsi.

– Kompyuter jinoyatlari bo‘yicha tezkor, jinoiy va sud amaliyoti.

– Tizim ishini tadqiq qilish usullari.

Umuman jinoyatchilikka forenzikaning ta’siri bir necha yo‘llar bilan bo‘lishi mumkin:

– axborot texnologiyalarining tez rivojlanishi kelajakda o‘zini yangi munosabatlari va yangi jinoyatlarini bilan ko‘rsatuvchi sun’iy ongni paydo bo‘lishini nazarda tutadi;

– yaqindagina axborot texnologiyalarining natijasi umuman qo‘riqlanmagan edi, hozirda vaziyat doimiy o‘zgarmoqda, masalan, domen nomi himoyalangan va intellektual mulk obyekti hisoblanadi;

– firibgarlik yo‘llari va tamoyillar o‘zgargan, biroq mohiyati o‘shaligicha qolgan: firibgarlikning ba’zi toifalari mohiyatini saqlab qoldi, biroq real muhitdan virtual muhitga o‘tdi.

Ilg‘or texnika va texnologiyalarning jinoyatchilikka ta’siri uch yo‘l bilan bo‘lishi mumkin:

Birinchidan, texnik progress jinoyatni yangi yo‘llar bilan va yangi qurollar yordamida sodir etish imkoniyatini beradi. Tabiiyki, shu yo‘sinda texnik progress jinoyatlarni fosh etishni yangi yo‘llarini paydo bo‘lishiga olib keladi – ham eskisini, ham yangisini. Masalan, o‘sha eski firibgarlik bizning asrda Internet tarmog‘i yordamida sodir etilmoqda. Biroq firibgarlikda dahl qilish predmeti va mohiyati o‘shaligicha qolmoqda. Yangilik faqat sodir etish quroli xolos – veb-sayt, elektron pochta, to‘lov tizimi.

Ikkinchidan, axborot texnologiyalarining natijalari jinoiy tajovuz qilish predmeti bo‘luvchi tamoyilan yangi ommaviy munosabatlarni paydo qiladi. Bunda tajovuz qilish yo‘li va quroli AT natijalarini hisobga olgan holda ham eski, ham yangi bo‘lishi mumkin.

Eng yorqin misol – domen nomi. Domen nomini berish huquqi kabi bunday ommaviy munosabat yaqingacha mavjud emas edi. Tajovuz qilish ham yo‘q edi. Hozirda domen nomi qonun bilan qo‘riqlanadi (ular intellektual mulk obyektiga kiritilgan).

Uchinchidan, AT rivojlanishi shunchaki yangi ommaviy munosabatlarnigina emas, balki bunday munosabatlarning yangi subyektini ham paydo bo‘lishiga olib kelishi mumkin. Kompyuter uchun dastur hali huquq subyekti sifatida qaralmayapti, biroq ba’zida tabiat kuchi sifatida qaralmoqda. Dasturlarga farovonlik va hattoki inson hayotiga sezilarli ta’sir qilishi mumkin bo‘lgan yechimlarni qabul qilish imkoni berilgan. Dasturlar allaqachon yangi mualliflik huquqi obyektlarini yaratishi mumkin. Tamoyilan yangi subyekt, o‘z huquqlari bilan jamiyatning yangi a’zosi – sun’iy intellekt paydo bo‘lishi yaqin. Uning paydo bo‘lishi yangi huquqiy munosabatlarni va mos holda yangi jinoyatlarni paydo bo‘lishiga olib keladi.

1.4. Kriminalistikani tadqiq qilish usullari

Ilmiy usullar ilm-fanning obyekti va predmetiga tegishli faoliyat turlari, jarayonlar, hodisalarni bilish yo‘llari hisoblanadi. Bunga mos kriminalistikani tadqiq qilish usullari – bu daliliy axborotlardan foydalanish, tadqiq qilish, yig‘ish namunalarini qabul qilish, qoidalar tizimidir.

Ularga o‘rganilayotgan hodisaning rostmana shartlarini o‘rnatish, uning xarakteri va ishtirokchilari bo‘yicha kriminalistik tavsiyalar ishlab chiqish yo‘llari, jinoiy ish bo‘yicha adolatli qaror qabul qilish taalluqli.

Kriminalistikani tadqiq qilish usullari **umumilmiy va maxsus usullarga** ajratiladi.

Umumilmiy usullar odatda nafaqat kriminalistikani tadqiq qilishda, balki fanning boshqa sohalarida ham foydalaniluvchi usullar tushuniladi. Asosiy umumilmiy usullarga avvalambor ***kuzatish, taqqoslash, umumlashtirish, ekstrapolyatsiya, tavsiflash, modellashtirish*** taalluqli.

Kuzatish hodisa, faoliyatni maqsadli qabul qilishdir. Kriminalistik tadqiqotlarda odamlar (ularning tashqi belgilari, u yoki bu harakatlarga reaksiyasi va shu kabilar); moddiy obyektlar (predmetlar, hujjatlar, izlar va ularning nusxalari); jinoyat ishtirokchilarining kriminal, postkriminal harakatlari (hodisa va jinoyat jarayonining boshqa ishtirokchilarini harakatlari); hodisalar (shakllanish jarayonlari va axborotni uzatish, uni turli bosqichlardagi transformatsiyasi va shu kabilar) kuzatiladi. Kuzatish jarayonida obyekt nafaqat bir butun, balki xossa, belgilar to‘plami kabi qabul qilinadi. Kuzatuv o‘z ichiga tadqiq qilinuvchi obyekt belgilar tizimini hissiy va ratsional bilishni birlashuvini oladi. Kuzatuv axborot aniqlangan turli ma’lumot tashuvchilar orqali amalga oshiriluvchi bevosita va bilvosita bo‘lishi mumkin.

Taqqoslash bir vaqtda bir nechta obyektlarni, har bir o‘rganilayotgan obyektlar xususiyatini solishtirish va ularning o‘xshashlik va farqlarini o‘rnatishdan iborat. Bu usulning o‘ziga xosligi obyektlar sifatini mosligi yoki farqini aniqlash nafaqat ajratilgan tadqiqot jarayonida, balki asosan bevosita solishtirishda amalga oshirilishidadir. Taqqoslash o‘xshashlik yoki farq haqida xulosa chiqariladigan umumiy belgilarga ega ikkitadan kam bo‘lmagan solishtiriluvchi obyektlar mavjudligida amalga oshirilishi mumkin. Taqqoslashning maqsadi tomonlarning aniq pozitsiyasi o‘rganilayotgan taqqoslanuvchi obyektlardagi umumiylikni aniqlash hisoblanadi. Ba’zi hollarda taqqoslash obyektni o‘ziga o‘xshash boshqa obyektlardan farqlanuvchi individual xususiyatlarni aniqlash maqsadida o‘tkaziladi.

Umumlashtirish birlashtiruvchi tendensiyalar, qonuniyatlar, aloqalarni o‘rnatish, belgilarning o‘xshashliklarini aniqlash yo‘li bilan yakkalikdan umumiylikka o‘tishdir. Umumlashtirish tahlil va sintez kabi mantiqiy harakatlar yordamida amalga oshiriladi. Tahlil murakkab obyektni yanada sodda elementlarga xayolan yoki faktga asosan bo‘lish, haqiqiylarini ajratishdir. O‘zaro bog‘liq aniqlangan umumiy belgilar bir butunga sintezlanadi. Umumlashtirishning natijasi kriminalistikaning deyarli barcha ilmiy tushunchalari va kategoriyalaridir.

Ekstropolyatsiya bir obyektning ma’lum belgilari, xususiyatlari borligi haqidagi xulosalarni boshqa predmetlar, hodisalar, jarayonlarga ko‘chirishdir. Ko‘chiriluvchi xulosalar o‘rganiluvchi obyektlar bilan o‘xshash o‘rganilgan obyektlarni kuzatishda shakllantiriladi. Masalan, psixologik izlanishlar jarayonida aniqlangan yolg‘on belgilari jinoiy jarayonda yolg‘on ko‘rsatmalarni o‘rganishda va ularni fosh etish harakatlarini ishlab chiqishda keng foydalaniladi.

Modellashtirish originalning belgilarini ma’lum to‘plamlarini akslantiruvchi xayoliy yoki moddiy analogni, ya’ni haqiqatdan ham mavjud moddiy obyekt, jarayon, harakatni yaratishdir. Natijada yaratiladigan model kriminalistikada o‘rganiladigan haqiqatda mavjud obyektlarni o‘z ichiga oladi. Tadqiqotni boshlang‘ich bosqichida bu obyektlar haqidagi ma’lumotlar to‘liqmasligi va ishonchni yetarlicha emasligi bilan xarakterlanadi. Vaziyat qatorida izlanuvchi ehtimoliy, gipotetik xarakterga ega asosli va argumentli fikrlash uchun axborotga ega emas.

Tavsiflash o‘rganiluvchi obyektning boshqa usullar orqali aniqlangan belgilarini fiksatsiyalash tushuniladi. Masalan, bevosita yoki bilvosita kuzatish, taqqoslash, umumlashtirish, tajriba va boshqalarda

aniqlangan belgilar tavsiflanadi. Ilmiy izlanishning bu usuli bir tomondan olingan bilimlarni ifodalash, bildirish vositasi, boshqa tomondan esa ularni tizimlashtirish vositasi hisoblanadi. Tadqiqot natijasida aniqlangan alohida obyektlarning belgilari avval tavsiflanadi, keyin esa umumlashtiriladi, toifalanadi. Tavsiflash yordamida olingan natijalar va ularning tushuntirishlari qo‘llaniladigan usullar, belgilar, obyektlar, texnologik jarayon, shartlar va tadqiqot ishtirokchilarini xususiyatlari fiksatsiyalanadi.

Maxsus usullar faqatgina kriminalistikada qo‘llaniladigan usullar bo‘lib, xususiy-kriminalistika va boshqa ilmlar ma’lumotlariga asoslangan usullarga ajraladi.

Birinchisiga odatda kriminalistik texnikalar sohasida tadqiqot o‘tkazishda foydalaniluvchi texnik-kriminalistik usullar kiradi. Masalan, hozirda yozuv psixologik xususiyatlari, hujjatlarni bajarishning psixik anomaliyalari, texnik vosita ishonchliligi yordamida baholash va so‘roq qilinayotganlarni obyektivligi hamda shu kabilar bo‘yicha diagnostika imkoniyatlari ustida tadqiqotlar olib borilmoqda.

Xususiy-kriminalistik usullarga mohiyati ma’lum tizimlarni qurishdan iborat tuzilmaviy kriminalistika usullari taalluqli. Bu usullarning tarkibi joriy axborotni qayta ishlash va yig‘ish bo‘yicha operatsiya va harakatlarni, ehtimoliy tuzilmalarni kengaytirish yo‘nalishlarini aniqlashni, amaliyotda foydalanish texnologiyalarini hosil qiladi.

1.5. Raqamli kriminalistika vositalari

Kriminalistikani rivojlanishi texnik va taktik harakatlarni aniq chegaralanishiga olib keldi. Buguni kunda «**kriminalistik texnika**» termini ikki ma’noda foydalaniladi: kriminalistikaning bir bo‘limi kabi va umumiy texnikaning sohasi kabi. Kriminalistik texnika kriminalistika ilmining tarkibiy qismi hisoblanib, turli texnik vositalar va usullar yordamida uning vazifalarini yechishni ta’minlashga yo‘naltirilgan.

Kriminalistik texnikaning asosiy vazifasi ko‘rinmas va noravshan izlarni aniqlash hamda chiqarib olish, izlanayotgan va daliliy axborotni olish, yashirish joylarni qidirishni osonlashtirish, jinoiy harakatlar amalga oshirilayotgan vaziyatni aniqlashni hujjatlashtirishning yuqori darajasini ta’minlash, tergovchi mehnatining samaradorligini oshirish imkoniyati hisoblanadi.

Kriminalistik amaliyotda aniqlashning turli vositalari qo‘llaniladi: fotoapparatlar, videokameralar, magnitofonlar va videomagnitofonlar, yopishqoq plyonkalar va boshqalar.

Kompyuter kriminalisti maxsus kriminalistik texnikasiz ham to‘liq ishlashi mumkin. Kompyuterning o‘zi yetarlicha universal quroldir. Turli qo‘shimcha va dasturiy ta’minotlar orasida funksiyani o‘rganish uchun kerakli barcha narsalar topiladi. Ba’zi dasturiy qurilmalarni osongina yaratish yoki o‘z qo‘llarimiz bilan modifikatsiyalashimiz mumkin.

Biroq maxsus texnika ishni juda yengillashtiradi. Bugungi kunda bozorda quyidagi kriminalistik qurollar mavjud:

– qattiq disklarni va boshqa ma’lumot tashuvchilarni klonlashtirish uchun qurilmalar;

– apparatli bloklangan yozish uchun o‘rganilayotgan disklarni ulash uchun qurilmalar;

– disklar va boshqa ma’lumot tashuvchilar, ularning tarkibini kriminalistik o‘rganish uchun dasturiy qurollar;

– kompyuter axborotini ish sharoitlarida o‘rganishga yo‘naltirilgan dasturiy va apparatli kompleks vositalarga ega ko‘chma kompyuterlar;

– o‘rganilayotgan fayl tizimlarini tarkibi filtrlash uchun xeshlarning to‘plami (hash sets);

– lokal tarmoqlarni o‘rganish uchun dasturiy vositalar;

– va ba’zi boshqa narsalar.

Apparat vositalari. Zamonaviy kompyuterlar universal qurilmaligini va ularda asosan ochiq standartlar va protokollar foydalanilishini hisobga olgan holda kompyuterlarni va kompyuter ma’lumot tashuvchilarini tadqiq qilish uchun maxsus apparat vositalari talab etilmaydi. Yani kompyuterning o‘zi universal instrument hisoblanadi, uning barcha funksiyalarini esa mos dasturiy vositalar orqali ishga tushirish mumkin.

Kompyuterlar va kompyuterning qo‘shimcha qurilmalari uchun apparat kriminalistik qurilmalar mutaxassis yoki ekspertga qulaylik uchun xizmat qiladi. Mobil telefonlar, raqamli fotoapparatlar va videokameralar, bort kompyuterlari, kommutatorlar, marshrutizatorlar, apparat tarmoqlararo ekranlar – bu barcha qurilmalar texnologik ochiq emas va universallikka intilishmaydi. Saqlanayotgan kompyuter axborotiga to‘liq ruxsat uchun har doim ham kompyuter va dasturiy instrument yetarli bo‘lavermaydi.

Ekspert dasturlar. Bunday dasturlar asosan ekspertiza o‘tkazish vaqtida kompyuter axborot tashuvchilarining tarkibini tadqiq qilishga

mo‘ljallangan. Ular nafaqat fayl tizimlari darajasida, balki pastroq darajada – qattiq disk kontrolleri darajasida ham ishlaydi, bu esa fayllarni o‘chirilgandan keyin ham qayta tiklash imkoniyatini beradi.

Bir nechta mashhur ekspert dasturlarini keltiramiz:

– ProDiscover dasturlar oilasi *(http://computer-forensics-lab.org/lib/ ?rid=22)*.

– SMART (Storage Media Analysis Recovery Toolkit) *(http://computer- forensics-lab.org/lib/?cid=18)*.

– «AccessData» firmasiga tegishli Forensic Toolkit (FTK) (*http://computer-forensics- lab.org/lib/?rid=26)*.

– Encase ekspert tizimi.

– ILook Investigator *(http://www.ilook"forensics.org)*.

– SATAN (System Administrator Tools for Analyzing Networks) – Unix OT uchun kompyuterlardan to‘liq axborotni olish uchun vosita.

– DIBS Analyzer 2 *(http://www.dibsusa.com/products/dan2.html)*.

– Helix – Linux OT asosidagi yuklanuvchi kompakt-diskdagi ekspert komplekt.

Xeshlar to‘plami. «hash sets» deb nomlanuvchi – xeshlar to‘plami asosan kompyuter qattiq disklarida katta axborot tashuvchilarning fayl tizimlarini tarkibini tadqiq qilishni osonlashtirish uchun mo‘ljallangan.

Faraz qilaylik, ekspertga o‘rganish uchun gumondordan tintuvda olingan operatsion tizim o‘rnatilgan va foydalanuvchi ma’lumotlari mavjud axborot tashuvchi vosita kelib tushdi. Bu ma’lumotlar turli direktoriyalar bo‘yicha tarqalgan bo‘lishi, sozlanmali fayllar ichida bo‘lishi, hattoki ko‘rinishidan umuman boshqa ma’lumotlardan iborat fayllar ichiga steganografiya usullari bilan yashirilgan bo‘lishi mumkin. Zamonaviy OT o‘z tarkibiga minglab fayllarni, mashhur ilovalarni – yuzlab va minglab olishi mumkin. Shunday qilib, oddiy kompyuterning fayl tizimida masalan, faqatgina 500 tasi foydalanuvchi tomonidan yaratilgan yoki o‘zgartirilgan 30000 ta fayllar bo‘lishi mumkin.

Bu foydalanuvchi fayllar «kamchiligini» hech qanday qiziq narsaga ega bo‘lmagan «ko‘pchilikdan» uzoqlashtirish uchun xeshlar to‘plami mo‘ljallangan.

Xesh, xesh-summa yoki bir tomonlama *xesh-funksiya* fayllari maxsus algoritm bo‘yicha fayl tarkibidan hisoblanuvchi uzun sondir. Xesh-summa nazorat summasiga o‘xshash, biroq bitta sezilarli farqi majud: bu bir tomonlama funksiya. Ya’ni fayl bo‘yicha osongina uning

xesh-funksiyasini hisoblash mumkin, biroq berilgan xesh-funksiyani terish orqali mos faylni olishning iloji yo‘q.

Ma’lum fayllarning xeshlari ularning tarkibini to‘liq ko‘rmasdan olib tashlash va bu fayllar foydalanuvchi axborotiga ega emasligiga ishonch hosil qilish imkonini beradi. Ular istisno qilingandan keyin ekspertga nisbatan kam sonli fayllarni tadqiq qilish qoladi xolos. Bunday to‘plam toifalari «knowngoods» deb nomlanadi.

Teskari vazifani bajaruvchi xeshlar to‘plami ham mavjud. Ular *«knownbads»* deb nomalanadi va zararsizligi oldindan no‘malum fayllarga, aksincha pornografiya, viruslar yoki boshqa kriminal kontentdan iborat aniq zararli fayllarga mos keladi. Odatda xeshlar to‘plami – bu muvofiq ishlab chiqaruvchidan sotib olinuvchi va ekspert DTga ulanuvchi alohida mahsulotdir. Bu fayllar haqidagi ma’lumotlarga mos keluvchi yuz minglab va millionlab xesh-funksiyalardan iborat bo‘lishi mumkin. Barcha mashhur ekspert tizimlari «tashqi» xeshlar to‘plamidan foydalanish va ulanish imkoniyatini beradi.

Arxivlash. Ilgari «zahira nusxalash» yoki «sovuq zahiralash» deb nomlanuvchi, ma’lumotlar nusxalarini nusxalash va uzoq vaqtli saqlash yo‘qotishda qayta tiklash maqsadidagina qo‘llanilgan.

So‘ngi paytlarda arxivlash boshqa maqsadlarda – bo‘lishi mumkin bo‘lgan yoki kelajakda aniqlanuvchi xavfsizlik insidentlarini tadqiq qilish uchun qo‘llanilmoqda. Ya’ni ma’lumotlar nusxalanishi «qimmatli, nozik ma’lumotlarning yo‘qotilishi zarar keltiradi» degan tamoyilda emas, balki umuman boshqa tamoyilda amalga oshiriladi: buzg‘unchi harakatlarining izlari qolishi mumkin bo‘lgan ma’lumot tashuvchilar va ma’lumotlar nusxalanadi. Masalan, xizmat shaxsiy kompyuteriga nisbatan qayta tiklash maqsadlari uchun foydalanuvchi fayllar va uning alohida sozlanmalari arxivlanadi. Operatsion tizimlar va amaliy dasturlar zahira tarzida nusxalanmaydi, chunki distributivdan osongina qayta tiklanadi. Barcha zahira nusxalash fayl tizimi darajasida amalga oshiriladi. Insidentlarni tadqiq qilish maqsadlari uchun kompyuterning barcha qattiq diski nusxalanadi, yana fayl tizimi darajasida emas, balki disk kotrolleri darajasida, ya’ni masofadagi va yashirish axborot kirishi uchun.

Zahira nusxasi insidentlarni tadqiq qilish uchun unchalik foydali emas. Aksincha, «insident» nusxasi virus hujumi yoki avariya vaziyatida qayta tiklash uchun to‘g‘ri kelmaydi. Bu turli nusxalar hisoblanadi – ham texnik, ham maqsadli. Insidentlarni tadqiq qilish holatida arxivlash uchun vosita – bu maxsus kriminalistik vositadir.

Kriminalistik fototasvir va videoyozuv.

Hozirgi vaqtda tergovchining ish joyida nafaqat kompyuter balki, maxsus dasturiy ta’minot, masalan, «Tergovchi AIJ» (AIJ – Avtomatlashtirilgan ish joyi) – tergov jarayonida ko‘plab axborot-analitik vazifalarni yechish imkonini beruvchi dastlabki tergov jarayonini axborot nuqtai nazaridan qo‘llab-quvvatlashni avtomatlashtirishga mo‘ljallangan individual texnik va dasturiy vositalar kompleksi bo‘lishi nazarda tutiladi.

Yangi texnologiyalar tergovchilarga kriminalistik ahamiyatli axborot manbalarini taqdim etadi, masalan, keng tarqalgan videokuzatuv kameralari yoki mobil telefon GSM-lokalizatsiyalari. Biroq zamonaviy axborot texnologiyalarining imkoniyatlarini milliy kriminalistlar tomonidan qo‘llanilmaydigan yoki yetarlicha samarali qo‘llanilmaydigan soha mavjud. Bu soha – jinoyat izlarini vizual aniqlash.

Kriminalistik fotografiya – kriminalistik texnikaning odatiy bo‘limlaridan biri; bir necha yil oldin olimlar kriminalistikada raqamli fotografiyadan foydalanishga qarshi edilar, biroq endi deyarli bu plyonkali fotografiyani chiqarib yubordi. Biroq texnologiyalar ilgariladi va turli jinoiy harakatlar amalga oshirilganda aniqlangan jinoyat izlarini aniqlashni yanada ravshan va aniqroq aniqlash imkoni bermoqda.

Bunday vositalar qatorida birinchi bo‘lib, videotasvirni aytish lozim. Ilmiy yoki o‘quv adabiyotlarida jinoyatni tadqiq qilganda kriminalistik videoyozuvni qo‘llash qandaydir harakatni, hodisa rivojlanish dinamikasini, ba’zida ovozlari bilan muhrlash muhim, bundan tashqari videoyozuv katta hududli maydonlarni yoki ko‘p tartibsiz to‘plangan turli obyektlarni muhrlash, ko‘rik davomida o‘zgartirilishi mumkin bo‘lgan, masalan, yong‘in va falokatlarda vaziyatni aniqlash imkonini beradi. Ya’ni fototasvir bilan solishtirganda videoyozuvning asosiy ustunlik tomoni muhitning o‘zgarish dinamikasini hamda statik bo‘lmagan harakatlanuvchi obyektlarni muhrlash imkoniyatidadir.

Videoyozuv – mos uslubni ishlab chiqishda jinoyat joyini ko‘rigi natijalari va qadamini aniq hamda to‘liq aniqlash imkonini beradi. Bundan tashqari statik predmetlarni, huquq buzilishini ehtimoliy o‘zgarish joyini, tashqi ta’sirsiz normal sharoitlarda statik vaziyatni aniqlashda videoyozuvning roli to‘g‘ri baholanmagan. Videoyozuv fototasvir kabi jinoyat joyini umuman yo‘naltirilgan, uzelli, umumiy va

batafsil ko‘rish, hamda alohida xususan jinoyat izlarini aniqlash imkoniyatini beradi.

Birinchidan, jinoyat joyini ko‘rigini tergovchi nuqtai-nazaridan, uni ko‘rikka bo‘lgan yondashuvidan amalga oshirish mumkin. Bu faqatgina tergov doirasida ko‘rik natijalarini keyingi tahlili uchungina muhim emas, balki agarda oqibatda tergovchi kompetenligi yoki harakatlarining qonuniyligiga shubha paydo bo‘lgan vaziyatda tergovchi harakatlarini baholash uchun ham muhimdir: agarda videoyozuvda qandaydir ashyoviy dalil olinishi va uni o‘rash aniqlansa, uni fosh etish yoki buzish yetarlicha qiyin bo‘ladi. Ikkinchidan, jinoyatchining jinoyat sodir etayotgandagi harakatlarini, uning jinoyat joyiga kelishini va qochish yo‘llarini video modellarini yaratish mumkin. Bunday modellarning keyingi tahlili yo‘naltiruvchi qiymatga ega bo‘lishi, jinoiy versiyalarni shakllantirish uchun xizmat qilishi, jinoyatchi yashiringan yoki kelgan joylarda yangi jinoyat izlarini aniqlashga yordam beradi. Uchinchidan, videoyozuv jinoyat joyiga kelib, jinoiy guruh kutmaydigan hodisalarni aniqlash imkonini beradi: zararlanishi boshida ravshan bo‘lmagan predmetlarni kutilmaganda qulashidan, jinoyat joyini tark etishga ulgurmasdan jinoiy guruhni ketishini kutib o‘tirishga umid qilib yashiringan jinoyatchini birdan paydo bo‘lib qolishigacha. To‘rtinchidan, hozirgi vaqtda jabrlanuvchi yoki guvohlarning xotiralarini tiklash yoki aktivizatsiyalash uchun jinoyat joyini ko‘rish vaqtida videoyozuvdan foydalanish imkoniyati hisobga olinmaydi, biroq oxirgi 20 yillikda xotirani aktivizatsiyalash mavzusi mutaxassislarning faol tadqiqot predmeti bo‘ldi.

3D-texnologiyalar. Jinoyat izlarini aniqlashni boshqa zamonaviy vositasi panoramali 3D-fotografiya hisoblanadi. Bunday fototasvir gorizontal va vertikal bo‘yicha 360° ni qamrab olishni imkonini beruvchi fotoapparatda maxsus nasadkadan foydalanish bilan amalga oshiriladi. Natijada monitor ekranida fotoapparat o‘rnatilgan nuqtadan hodisa joyini to‘liq tasvirini olish mumkin. Panoramaning alohida qismlarini yanada batafsil ko‘rish uchun yaqinlashtirish mumkin. Bunday tasvirlar alohida detallarni shunchaki aniqlashdan ko‘ra ko‘proqdir. Bular tergovchi tomonidan ham jinoyat joyini keyingi tahlil uchun va yangi izlarni qidirish uchun, ham ko‘rsatma beradigan shaxslarni xotirasini aktivizatsiyalash uchun foydalanilishi mumkin.

Bundan tashqari, jinoyat hodisasini bir nechta odam (ularning keyingi protsessual statusi turlicha bo‘lishi mumkin) kuzatganda ham turli nuqtai nazardan hattoki ular aynan nimani ko‘rishganini

anglayolmay qolganda bunday fototasvirdan foydalanish eng samarali hisoblanadi. Barcha guvohlarning nuqtai-nazarida panoramali 3D-fotografiyalarni yaratish va ularni keyingi birgalikdagi tahlil ko‘rimaydigan zonalarni, ya’ni kimningdir yoki birdaniga barcha guvohlarning ko‘ziga ko‘rinmay qolgan hududlarni aniqlash imkonini beradi. Shunday qilib, bir tomondan ko‘rsatmalarni ishonchliligini tekshirish – guvoh ko‘rganini tasdiqlayotganda u yoki bu predmet yoki hodisani ko‘rishi mumkin emasligini isbotlash.

Panoramali 3D-fotografiyalarni bunday solishtirish kompyuter modellashtirishni, maxsus dasturiy ta’minotni va maxsus bilimlarni talab qiladi, solishtirish natijalari esa har bir guvohning ko‘rish zonalarini ko‘rsatuvchi yaqqol model, kesishuvchi ko‘rish zonalari, ko‘rinmas zonalardan iborat bo‘lishi lozim. Ya’ni bunday solishtirish sud ekspertizasi shaklida amalga oshirilishi kerak.

Jinoyat izlarni aniqlashning yana bir vositasi *lazerli 3D-skanerlash* hisoblanadi. Hozirda bu usul AQSH va G‘arbiy Yevropada yetarlicha faol qo‘llanilmoqda; fiksatsiyaning bunday vositasini qo‘llash yaqin kelajak amalidir, bu yerda yagona to‘siq – qurilmaning nisbatan yuqori narhi va tergovning adekvat vazifalari bo‘lib, jinoyat joyini 3D-fiksatsiya usulini yo‘qligidir.

3D-model ish bo‘yicha ko‘rsatma beruvchi shaxslar bilan ishlash uchun, ularni xotirasini aktivizatsiyasi uchun, hamda tavsiflangan vazifalar, ham turli toifadagi modellashtirish – o‘q trayektoriyalari, hodisa ishtirokchilarining harakat sxemalari, hodisalarni rivojlanishini ehtimoliy ssenariylari va shu kabilar bilan bog‘liq turli kompyuter-texnik ekspertizalarini o‘tkazish uchun to‘g‘ri keladi. Lazerli skanerlash yordamida olingan model ko‘rsatmalarni tasdiqlash yoki bo‘liqlarni to‘ldirish uchun ham ishlatilishi mumkin: modeldan hodisa joyining alohida detallarini olib tashlab yoki jinoyat joyida ko‘rik natijalari va kechishini fiksatsiyalash vaqtida oldindan qandaydir predmetlar bo‘lmaganligi, masalan, ular jinoyatchi tomonidan o‘g‘irlangan, jinoyat joyiga birinchi kelgan shaxslar tomonidan yashirilgan va shu kabilarni taxmin qilib, ko‘rsatmalari tekshirilayotgan shaxsga yuzlarni taklif qilishi, modelni dasturiy ta’minotning bir qismi bo‘lgan obrazlar kutubxonasidan tanlash mumkin bo‘lgan yetmayotgan predmetlar bilan to‘ldirish mumkin.

Virtual reallik. Bundan tashqari keyingi tadqiqot uchun istiqbolli yo‘nalishlardan biri hodisa joyida bo‘lish effektini yaratuvchi monitor ekranidan virtual reallikka ko‘chish modelidir.

Virtual hodisa joyini yaratish va undan foydalanish uchun maxsus dasturiy ta’minot va virtual reallik shlemi kerak. Bunday virtual modeldan foydalanish ish bo‘yicha ko‘rsatma berayotgan shaxslar bilan ishlash uchun samaralidir. Birinchidan, virtual reallik sharoitlarida hodisa joyini qabul qilish yorqinligi foto- yoki video-tasvirdan ko‘ra inson xotirasiga kuchli ta’sir ko‘rsatadi. Ikkinchidan, hodisa joyini virtual modeli lazerli 3D-skanerlash natijasida olingan batafsil tasvirni hisobga olgan holda va hodisa joyini dastlabki ko‘rigiga hamrohlik qiluvchi barcha shartlarni saqlash joyda ko‘rsatmalarni tekshirish uchun foydalanilishi mumkin. Bugungi kunda joydagi ko‘rsatmalar tekshiruvi jinoyatdan sezilarli vaqt o‘tgandan keyin hodisa joyidagi vaziyat allaqachon buzilganda o‘tkaziladi. Virtual model birinchi ko‘rik momentida qanday bo‘lgan bo‘lsa o‘shanday hodisa joyida qayta bo‘lish imkonini beradi. Biroq so‘zsiz bu tadbir xususiy jinoiy harakat deb hisoblanishi mumkin emas.

Shunday qilib, jinoyat izlarini vizual fiksatsiyalash texnologiyalari va yangi vositalaridan foydalanish jinoyatlarning to‘liq tergov qilish va o‘z vaqtida fosh etish uchun katta ahamiyatga ega.

Kriminalistik axborot tizimlari.

Ko‘rsatilgan tizimlar to‘g‘ridan-to‘g‘ri dalillarni o‘rganish va izlash uchun foydalanilmaydi. Ular jinoyatlarni fosh etish va tergov qilish bo‘yicha ishlarda ta’minot funksiyasini bajaradi. Biroq odatiy kriminalistik texnikaga tallluqli. Kriminalistik axborot tizimlari bir qator bir-biriga yaqin vazifalarni bajaradi:

– tezkor-qidiruv tadbirlari (TQT), dastlabki oqibatlar, sud maqsadlari uchun turli hujjatlarni rasmiylashtirishni yengillashtiradi va/yoki tezlashtiradi;

– huquq tartibot organlari xodimlariga kerakli akt, izohlar, maslahatlar olishni tezroq topish imkonini beradi;

– xodimlarga ham ommaviy, ham yopiq bo‘lgan barcha ma’lumotlar bazasi, hisoblar, qo‘llanmalarga ruxsatni yengillashtiradi va tezlashtiradi;

– xabarlarni ushlab olish bilan bog‘liq TQTni o‘tkazishni avtomatlashtiradi va tezlashtiradi.

Mutaxassislar va ekspertlar o‘tkazadigan kriminalistik jarayonlarni to‘rt bosqichga ajratish qabul qilingan:

1) yig‘ish;

2) tadqiq qilish;

3) tahlil;

4) taqdim qilish.

Birinchi bosqichda axborotning o‘zi hamda kompyuter axborotining tashuvchisini yig‘ish amalga oshiriladi. Yig‘ish atributlash (belgilash), manbalarni ko‘rsatish va ma’lumotlar va obyektlarni kelib chiqishi bilan birga amalga oshirilishi lozim. Yig‘ish jarayonida axborotning saqlanganlik va butunliligi (o‘zgarmaslik) ba’zi hollarda esa maxfiyligi ham ta’minlanishi lozim. Yig‘ishda ba’zida qisqa vaqtli axborotni aniqlash uchun maxsus choralarni ko‘rishga to‘g‘ri kelinadi, masalan, joriy tarmoq ulanishlarini yoki kompyuter tezkor xotirasining tarkibini.

Ikkinchi bosqichda yig‘ilgan axborotning (tashuvchi-obyektlarning) ekspert tadqiqi o‘tkaziladi. Bu o‘z ichiga axborot tashuvchilarda axborotni olish/hisoblashni, dekodlash va undan ishga aloqadorini ajratishni oladi. Ba’zi tadqiqotlar u yoki bu darajada avtomatlashtirilishi mumkin. Biroq bari bir ekspert bu bosqichda boshi va qo‘li bilash ishlashiga to‘g‘ri keladi. Bunda o‘rganilayotgan tashuvchilardagi axborot butunliligi ta’minlanishi kerak.

Uchinchi bosqich tanlab olingan axborot ekspert yoki mutaxassis oldiga qo‘yilgan savollarga javob olish uchun tahlillanadi. Tahlilda faqatgina ishonchliligi tasdiqlangan ilmiy usullardan foydalanilishi kerak.

To‘rtinchi bosqich o‘z ichiga tadqiqot natijalarini mutaxassis bo‘lmagan shaxsga tushunarli shaklda rasmiylashtirish hamda o‘rnatilgan qonun bo‘yicha tahlilni oladi.

1.6. Kontr-forenzika

Raqamli dalillarni izlash, aniqlash va mustahkamlash usullariga qarshilik forenzikaning o‘zidek faol rivojlanmayapti. Qarshi usullariga bo‘lgan talab cheklangan. Nimaga cheklangan? Buni tushunish uchun kompyuter axborotini aniqlashga qarshilik qilish kimga va nima uchun kerak bo‘lishini ko‘rib chiqamiz.

Birinchidan, dastlab xayolga – ***kiberjinoyatchilar*** keladi. O‘zining kriminal harakatlarining izlarini yashirish va qonundan qo‘rqish asosiga ega shaxslar. Tushunarliki, bu bozor juda tor, unda ishlash juda qiyin, ulkan yuqori texnologiya kompaniyalari talab bo‘lsa ham bu segment uchun qurilmalar va DT ishlab chiqarishi amri mahol.

Ikkinchidan, qarshi usullar axborotni himoyalashning tarkibiy qismidir. Maxfiy axborotni himoyalashga ehtiyoj bor barcha joyda uning chiqib ketishini oldini olish uchun bu usullardan foydalanishi kerak. Chiqib

ketish bilan kurashish bo‘yicha bu usullarning bir qismi raqib axborotini istisno yoki uni qayta tiklashni qiyinlashtirishga yo‘naltirilgan.

Uchinchidan, fuqarolarning shaxsiy hayot siriga huquqi (yashirinlik) kompyuter-texnik va boshqa choralar qatorida ta’minlanishi mumkin, bu deyarli ***kriminalistikaga qarshi (kontr-kriminalistik)*** choralar hisoblanadi. To‘g‘ri, ko‘rsatilgan fuqarolarning shaxsiy hayot siriga huquqi himoyalash o‘rta foydalanuvchi malakasi bilan cheklanganligi sababli juda murakkab vositalar va usullarni qo‘llashning bu yerda iloji yo‘q.

Bu usullar AT sohasida yuqori malakani talab eta olmaydi, mos dasturlar boshqaruvda sodda bo‘lishi va «Windows» OT da ishlashi kerak, qurilmalar ham qimmat bo‘lishi kerak emas. Shuning uchun ham bu yerda odatda yetarlicha sodda himoya bilan cheklaniladi.

Ko‘rinib turibdiki, anti-kriminalistik texnikaning sezilarli qismi professional, hech ham oddiymas. Ko‘rinib turganidek, anti-kriminalistik bozor sezilarli darajada kriminalistik bozordan kichik. Anti-kriminalistik mahsulot sifatsiz bo‘lib chiqsa, ishlab chiqaruvchiga da’vo qila olmaysiz. Bu bozorda ilgarilash uchun umuman sifatli, murakkab qurilma va DT ishlab chiqish talab etilmaydi. Shunchaki o‘z mahsulot yoki xizmatingizni yaxshi reklama qilish talab etiladi xolos. Ishlab chiqaruvchilar shu bilan shug‘ullanishadi.

Himoyali anti-kriminalistik vositalarga quyidagilarni kiritish mumkin:

– saqlanuvchi axborotni shifrlash uchun dasturiy va apparat-dasturiy qurilma;

– trafikni shifrlash uchun dasturiy va apparat-dasturiy qurilma;

– disk va boshqa axborot tashuvchilarni tozalash uchun dasturlar;

– axborotni o‘chirish uchun dasturlar;

– magnitli tashuvchilarda axborotni mexanik yo‘q qilish uchun qurilma;

– diskda axborotni borligini yashirish uchun dasturlar (fayl atributlarini manipulyatsiyasi, nostandart joylarga yozish, stegenografiya);

– tarmoq faolligini anonimlashtirish uchun tizimlar va xizmatlar;

– raqamli shaklda taqdim etilgan asarlarni nusxalashni qiyinlashtirish uchun dasturiy va apparat-dasturiy qurilmalar;

– dastur algoritmlari va bajariluvchi kodlarini tadqiq qilinishini qiyinlashtirish uchun dasturlar.

Asosiy xulosalar

Raqamli kriminalistika – bu jinoyatlarni (insidentlarni) tadqiq qilish va kompyuterlarda, ma’lumotlarni saqlash tizimlarida, kompyuter tarmoqlarida, mobil va boshqa raqamli qurilmalarda joylashgan raqamli dalillarni yig‘ish haqidagi, kompyuter axboroti shakliga (raqamli dalillar) ega dalillarni tadqiq qilish va olish usullari haqidagi, buning uchun qo‘llaniluvchi texnik vositalar haqidagi amaliy fandir.

Raqamli kriminalistikaning vazifasi raqamli dalillarni saqlash, identifikatsiyalash, olish va hujjatlashtirish hisoblanadi.

Forenzikani qo‘llash sohasi: kompyuter axboroti tajovuz qilish obyekti, kompyuter esa jinoyatni sodir etish quroli kabi shakllanuvchi hodisalarni tergov qilish va tahlillash.

Kompyuter jinoyatining 3 yo‘nalishi ajratilib ko‘rsatiladi: axborot xavfsizligiga qarshi jinoyat; elektron axborot boshqa jinoyatni sodir etish vositasi hisoblanuvchi jinoyat; kompyuter va boshqa elektron texnikadan foydalanilib sodir etiladigan jinoyat.

Raqamli kriminalistikaning ko‘rinishlari: kompyuter kriminalistikasi, tarmoq kriminalistikasi, mobil kriminalistika.

Raqamli kriminalistikaning vazifalari: tezkor-qidiruv tadbirlari (TQT) va kompyuter axboroti bilan bog‘liq jinoiy harakatlarni taktikasini ishlab chiqish; kompyuter jinoyatining dalillarini tergov qilish va yig‘ish uchun apparat va dasturiy instrumentlar, usullarni yaratish; kompyuter axboroti bilan bog‘liq qoidabuzarliklarni kriminalistik xarakteristikasini o‘rnatish.

Raqamli kriminalistika predmetlari: axborot texnologiyalari, amaliy dasturiy ta’minotni o‘rganish usullarini, kompyuter jinoyati bo‘yicha kriminal, tezkor, jinoiy va sud amaliyoti, tizim ishini tadqiq qilish usullari.

Kriminalistikaning tadqiq qilish usullari umumilmiy (kuzatish, tavsiflash, taqqoslash, umumlashtirish, ekstropolyatsiya, modellashtirish) va maxsus usullarga (xususiy-kriminalsitik va boshqa ilm ma’lumotlariga asoslangan) ajraladi.

Kompyuter kriminalisti maxsus kriminalistik texnikasiz ham ishlashi mumkin. Kompyuterning o‘zi yetarlicha universal instrument. Biroq maxsus texnika ishni juda yengillashtiradi.

Kriminalistik axborot tizimlari TQT uchun turli hujjatlarni rasmiylashtirilishini tezlashtiradi va/yoki osonlashtiradi; kerakli meyoriy aktlarni, izohlarni topishni, maslahat olishlarni tezlashtiradi; ham ommaviy, ham yopiq barcha ma’lumotlar bazasi, hisoblar,

qo‘llanmalarga ruxsatni tezlashtiradi va osonlashtiradi; xabarlarni ushlab olish bilan bog‘liq TQT o‘tkazilishini avtomatlashtiradi va tezlashtiradi.

Kontr-forenzika – bu raqamli dalillarni qidirish, aniqlash va mustahkamlash usullariga qarshi usullardir. Anti-kriminalistik texnikaning sezilarli qismi – professional emas, lekin sodda ham emas. Anti-kriminalistik bozor sezilarli darajada kriminalistik bozordan kichik.

Nazorat uchun savollar

1. *«Forenzika» iborasi nimani anglatadi?*
2. *Raqamli kriminalistikaning asosiy vazifalari.*
3. *Kompyuter jinoyatining uchta yo‘nalishini ayting.*
4. *Raqamli kriminalistikaning ko‘rinishlarini keltiring.*
5. *Raqamli kriminalistikaning predmeti nima?*
6. *Forenzikaning qo‘llanilish sohalarini sanab o‘ting.*
7. *Axborot vositalarini qo‘llagan holda sodir etiladigan jinoyat guruhlarini shakllantiring.*
8. *Texnik va huquqiy xarakterdagi muammolarni hisobga olgan holda raqamli kriminalsitika qanday vazifalarni yechadi?*
9. *Ilg‘or texnika va texnologiyalarning natijalari jinoyatchilikka qanday ta’sir qiladi?*
10. *Kriminalsitikani tadqiq qilish usullarini ayting.*
11. *Raqamli kriminalistika maxsus texnik vositalarini xarakterlang.*
12. *Raqamli kriminalistikada ekspert dasturlar nima uchun mo‘ljallangan?*
13. *Kriminalistik fototasvir va videoyozuvni mohiyatini oching.*
14. *Kriminalistik axborot tizimlarining vazifalari.*
15. *Kontr-forenzika tushunchasini shakllantiring.*

2. KOMPYUTER JINOYATLARI

2.1. Kompyuter jinoyatlarining asosiy yo‘nalishlari

90-yillarning boshlaridan xorijiy huquqni muhofaza qilish organlari faoliyatida tez-tez **«computercrime» - kompyuter jinoyati** kabi ibora uchrab turadi, ya’ni kompyuterdan foydalanish bilan bog‘liq jinoyat.

«Kompyuter jinoyati» iborasi *«kompyuter axboroti sohasidagi jinoyat»* dan ko‘ra kengroq. Yana bu soha kompyuter texnikasi, dasturlar, kompyuter axboroti va raqamli aloqa kanallari jinoyatni sodir etish quroli yoki tajovuz qilish obyekti hisoblanadigan jinoyatlarni ham qamrab oladi. Bunday jinoyatlarga quyidagilar taalluqli: bank kartalarini qo‘llagan holdagi firibgarlik **(karding)**, shaxsiy ma’lumotlarni olish bilan bog‘liq firibgarlik **(fishing)**, aloqa xizmatlaridan noqonuniy foydalanish va aloqa sohasidagi boshqa yolg‘onlar **(frod, trafikni o‘g‘irlash)**, obyekt axborot tizimi hisoblanuvchi sanoat va boshqa josuslik va shu kabilar.

Fosh etish uchun kompyuter kriminalistikasi usullaridan foydalaniladigan har qanday jinoyatni kompyuter jinoyati deyish mumkin. Xorijiy adabiyotlarda va boshqa rasmiy hujjatlarda «computer crime» o‘rniga tez-tez «cybercrime» - kiberjinoyatchilik, kiberjinoyat iboralari foydalaniladi.

Ko‘pincha quyidagi iboralar ishlatiladi:

Kompyuter jinoyati (kiberjinoyat) – tadqiq uchun tabiiy shart axborot texnologiyalari sohasida maxsus bilimlarni qo‘llash hisoblanadigan ma’muriy huquqbuzarlik.

Kompyuter va kompyuter axboroti kompyuter jinoyatida uchta rolni o‘ynashi mumkin:

- tajovuz qilish obyekti;
- sodir etish quroli;
- dalil yoki dalil manbasi.

Barcha uchta holatda dalillarni aniqlash, yig‘ish, aniqlash va tadqiq qilish uchun maxsus bilim va maxsus usullar talab etiladi.

Axborot xavfsizligini ta’minlash muammosi insonlar axborot bilan almashinishni, to‘plashni va saqlashni boshlagan vaqtdan dolzarb hisoblanadi. Har doim insoniyatning muhim yutuqlarini ishonchli saqlash zarurati paydo bo‘lgan. Analog tarzida maxfiy axborot almashinuvi va uning ishonchli himoyasiga zarurat paydo bo‘lgan.

Kompyuter jinoyati – jinoyat kodeksida koʻrsatilgan mashina axboroti jinoiy tajovuz qilish obyekti hisoblanadigan jamiyat uchun xavfli harakatdir. Joriy holatda jinoyat predmeti yoki quroli sifatida mashina axboroti, kompyuter, kompyuter tizimi yoki kompyuter tarmogʻi xizmat qiladi.

Kompyuter jinoyatini shartli ravishda ikkita katta kategoriyaga ajratish mumkin:

– kompyuter ishiga aralashish bilan bogʻliq jinoyat;

– kompyuterni kerakli texnik vosita kabi foydalaniladigan jinoyat.

Kompyuter ishiga aralashish bilan bogʻliq jinoyat asosiy koʻrinishlarini sanab oʻtamiz.

1) Axborotga Ruxsatsiz kirish (RK). RK begona nomdan foydalanish, texnik qurilmalarning fizik manzillarini oʻzgartirish, vazifa yechilgandan keyin qolgan axborotdan foydalanish, dasturiy va axborot taʼminotni modifikatsiyalash, axborot tashuvchini oʻgʻirlash, maʼlumotlarni uzatish kanallariga ulanadigan yozuv apparaturalarini oʻrnatish bilan amalga oshiriladi.

Xaker, «kompyuter qaroqchisi» - koʻngilxushlik, firibgarlik yoki zarar yetkazish (kompyuter virusini tarqatish yoʻli bilan ham) maqsadida kompyuter tizimlari va tarmoqlariga tizimli ruxsatsiz kirishni amalga oshiruvchi shaxsdir. Bir tomondan «xaker» - kompyuterni yaxshi biladigan va yaxshi dasturlarni yozuvchi shaxs boʻlsa, boshqa tomondan axborotni olish maqsadida kompyuter tizimlariga noqonuniy kiruvchi shaxsdir.

Ingliz feʼli «to hack» kompyuterlarga qoʻllanilganda ikki maʼnoni anglatishi mumkin – tizimni buzish yoki uni tuzatish. Bu harakatlar asosida qandaydir umumiylik mavjud – kompyuter va unda ishlaydigan dasturlar qanday tuzilganligini tushunish.

Shunday qilib, «xaker» soʻzi ikki maʼnoga ega: birinchisi – negativ boʻyalgan («buzgʻunchi»), boshqasi – neytral yoki maqtanarli («usta», «master»). Boshqa soʻzlar bilan aytganda xakerlarni «yomon» va «yaxshi» xakerlarga ajratish mumkin.

«Yaxshi» xakerlar texnik progresga hissa qoʻshishadi va oʻzlarining bilim va koʻnikmalarini insoniyat rivoji uchun ishlatishadi. Ular tomonidan katta miqdordagi yangi texnik va dasturiy tizimlar ishlab chiqilgan. Ularga «yomon» xakerlar qarshilik qilishadi: boshqalarning xatlarini oʻqishadi, boshqalarning kodlarini oʻgʻirlashadi va insoniyat rivojiga barcha yoʻllar orqali zarar yetkazishadi.

«Yomon» xakerlarni shartli ravishda to‘rt guruhga ajratish mumkin.

Birinchi guruh – **qiziquvchilar**, asosan yoshlardan iborat, kompyuter tizimlarini shunchaki ko‘ngilxushlik uchun buzuvchi insonlar. Ular zarar keltirishmaydi, bunday mashg‘ulot o‘zlari uchun foydali – vaqt o‘tgan sari ulardan yaxshi kompyuter mutaxassislari yetishadi.

Ikkinchi guruh – **qaroqchilar.** Ular kompyuter himoyasini yangi dasturlarni va boshqa axborotni o‘g‘irlash uchun buzishadi.

Uchinchi guruh – **xakerlar**, o‘z bilimlarini haqiqatdan ham har bir kishiga va hammaga zarar yetkazish uchun foydalanishadi. Ular kira olgan kompyuter tizimlarini yo‘q qilishadi, begona xatlarni o‘qishadi, keyin esa ularning mualliflari ustidan kalaka qilishadi. Telekonferensiyalarda ularning buzib kirishlari haqidagi hikoyalarini o‘qiganingizda bu insonlar o‘z g‘ururlarini haqoratlagan hisli insonlardek tuyuladi. Yana bir guruh bor – kimlarnidir buyurtmalari bo‘yicha maxfiy axborotni olish uchun ov qiluvchi xakerlar.

Xakerliklar orasida to‘rt asosiy toifa ajralib turadi.

Birinchi – ***romantik-yakkalar.*** Ular ma’lumotlar bazasini shunchaki qiziqishga buzishadi. Umuman ular xavfsiz va beg‘araz, biroq ancha qobiliyatli. Shuning uchun ham qandaydir firmaning kompyuter tarmog‘ini massali buzish odatda «romantiklar»dan biri zarar yetkazish va buni o‘z tarmog‘ida maqtanish bilan boshlanadi.

Ikkinchi – ***pragmatiklar yoki klassiklar.*** Bir o‘zlari ham, guruhda ham ishlashadi. Nima kelsa o‘g‘irlashadi – o‘yinlar, dasturlar, turli xildagi nashrlarning elektron versiyalari.

Uchinchi – ***razvedkachilar.*** Hozirda o‘zini hurmat qilgan har qanday firma dasturchi kabi rasmiylashtirilgan xakeriga ega. Uning vazifasi – raqiblarining tarmog‘ini buzish va u yerdan turli axborotni o‘g‘irlash. Bu toifa hozirda juda talabgir hisoblanadi.

To‘rtinchi – ***kibergangsterlar.*** Bular professional kompyuter buzg‘unchilar. Ularning vazifasi kompyuter tarmoqlarini aniq - blokirovkalash va ishini buzish, hamda bank hisob raqamlaridan pullarni o‘g‘irlash. Bu ish qimmat va xavfli, lekin yuqori haq to‘lanadi.

2) Dasturiy ta’minotga «mantiqiy bombalar»ni kiritish. Ular ma’lum vaqtda ishga tushadi va qisman yoki to‘liq kompyuter tizimini ishdan chiqaradi.

«Vaqt bombalari» - ma’lum vaqt momentida ishga tushadigan «mantiqiy bombalar»ning bir turi.

*«Troyan otlari»*ning usuli dastur egalari rejalashtirmagan, yangi funksiyalarni amalga oshirish imkonini beruvchi, biroq shu vaqtning o‘zida oldingi ishlash qobiliyatini saqlovchi komandalarni begona dasturga yashirin holda kiritishdan iboratdir. «Troyan oti» yordamida jinoyatchilar masalan, o‘zlarining hisobiga har bir operatsiyadan ma’lum summani o‘tkazishadi.

«Troyan otlari»ning yana bir turi mavjud. Ularning qobiliyati shundan iboratki, aynan «qora» ishni bajaradigan zararsiz dasturining bir qismi kabi ko‘rinadigan komandalar emas, balki bu komandalarni shakllantiruvchi keyin esa ish bajarilgach ularni o‘chiruvchi komandalar qo‘yiladi. Bu holda «troyan oti»ni topishga urinadigan dasturchi uni o‘zini emas, balki uni shakllantiruvchi komandani izlashi kerak. Bu g‘oyani rivojlantirib, komandalarni yaratuvchi komandalarni va keyinchalik «troyan oti»ni yaratuvchi komandalarni tasavvur qilish mumkin (qancha bo‘lsa shuncha marta).

3) Kompyuter viruslarini tarqatish va ishlab chiqish.

4) Dasturiy-hisoblash komplekslarini ishlab chiqish, tayyorlash va ekspluatatsiya qilishda jinoiy ehtiyotkorsizlik. Kompyuter ehtiyotkorsizligining o‘ziga xosligi shundaki, tamoyilan xatosiz dasturlarning bo‘lmasligidadir. Agarda loyihani texnik sohaning deyarli istalgan sohasida ulkan ishonch bilan bajarib bo‘lsa, unda dasturlash sohasida bunday ishonchlilik shartli, bir qator hollarda esa deyarli yetib bo‘lmasdir.

5) Kompyuter axborotini qalbakilashtirish. Kompyuter jinoyatchiligining bunday ko‘rinishi eng yangilaridan hisoblanadi. Bu ruxsatsiz foydalanishning bir turi hisoblanib, farqli jihati tashqi foydalanuvchi emas, balki yetarlicha yuqori malakaga ega ishlab chiqaruvchi foydalanishi mumkin. Jinoyatning g‘oyasi tarkibiy qismi kompyuter hisoblanuvchi katta tizimlarning ishlash ishga yaroqlilik holatini imitatsiyalash maqsadida kompyuterning chiquvchi axborotlarini qalbakilashtirishdan iborat. Yetarlicha ustalik bilan bajarilgan qalbakilashda buyurtmachiga nosoz mahsulotni berish muvaffaqiyatli amalga oshadi. Axborotni qalbakilashtirishga saylov, ovoz berish, referundumlar va boshqa natijalarni qalbakilashtirish ham kiradi. Agarda har bir ovoz beruvchi uning ovozi to‘g‘ri ro‘yhatga olinganligiga ishonch hosil qilmasa, unda har doim natijaviy protokollarga buzilishlarni kiritish mumkin.

6) Kompyuter axborotini o‘g‘irlash. Agarda «oddiy» o‘g‘irlash mavjud jinoiy qonunlar ostiga tushsa, unda axborotni o‘g‘irlash

muammosi ancha murakkab hisoblanadi. Mashina axborotini, dasturiy ta’minotni ham ruxsatsiz nusxalash yo‘li bilan o‘zlashtirish o‘g‘irlash deb hisoblanmaydi, chunki, o‘g‘irlash degani tashkilot fondidan boyliklarni olish bilan bog‘liq. Mulkka noqonuniy munosabatda bo‘lishda mashina axboroti fondlardan olinmasdan nusxalanishi mumkin.

2.2. Kompyuter jinoyatlarining klassifikatsiyasi

Xorijiy mutaxassislar tomonidan kompyuter jinoyatchiligini sodir etish yo‘llarining turli klassifikatsiyalari ishlab chiqilgan. Quyida Bosh Interpol Sekretariati kodifikatoriga to‘g‘ri keladigan jinoyatlarni sodir etish yo‘llarini nomlari keltirib o‘tilgan. 1991 yilda joriy kodifikator avtomatlashtirilgan qidiruv tizimiga integratsiyalangan edi va hozirda 100 dan ortiq davlatlarda Milliy markaziy byuro (MMB) mavjud.

Kompyuter jinoyatlarini xarakterlovchi barcha kodlar Q harfi bilan boshlanuvchi identifikatorlarga ega. Jinoyatlarni xarakteristikasi uchun sodir etilganlarni ahamiyatliligiga qarab kamayish tartibida joylashtirilgan beshta kodlargacha foydalanilishi mumkin.

QA - Ruxsatsiz kirish va ushlab olish:
QAH – *kompyuterni egallash,*
QAI – *ushlab olish,*
QAT – *vaqtni o‘g‘irlash,*
QAZ - *ushlab olish va ruxsatsiz kirishning boshqa ko‘rinishlari.*

QD – Kompyuter ma’lumotlarini o‘zgartirish:
QDV – *kompyuter virusi,*
QDT – *troyan otlari,*
QDW – *kompyuter chuvalchanglari,*
QDZ – *ma’lumotlarni o‘zgartirishning boshqa ko‘rinishlari.*

QF – Kompyuter firibgarliklari:
QFC – *bankomatlar bilan bog‘liq firibgarliklar,*
QFF – *kompyuter qalbakilashtirilishi,*
QFG – *o‘yin avomatlari bilan bog‘liq firibgarliklar,*
QFM – *kiritish-chiqarish dasturlari firibgarliklari,*
QFP – *to‘lov vositalari firibgarliklari,*
QFT – *telefon firibgarliklari,*
QFZ – *boshqa kompyuter firibgarliklari.*

QR – Noqonuniy nusxalash:
QRG – *kompyuter o‘yinlari*,
QRS – *boshqa dasturiy ta’minotlar*,
QRT - *yarimo‘tkazgich mahsulotlari topografiyasi*,
QRZ - *boshqa noqonuniy nusxalashlar.*

QS – Kompyuter ishini buzish:
QSH – *apparat ta’minoti bilan*,
QSS – *dasturiy ta’minot bilan*,
QSZ – *buzishning boshqa ko‘rinishlari.*

QZ – Boshqa kompyuter jinoyatlari:
QZB - *kompyuter e’lonlar doskalaridan foydalanilgan holda,*
QZE - *tijoriy sirni saqlovchi axborotni o‘g‘irlash,*
QZS - *maxfiy xarakterdagi axborotni uzatish,*
QZZ - *boshqa kompyuter jinoyatlari.*

Keltirilgan kodifikator mos holda kompyuter jinoyatlarini ba’zi ko‘rinishlarini qisqacha xarakterlaymiz.

Axborotni ushlab olish va ruxsatsiz foydalanish (QA) quyidagi kompyuter jinoyatlarining ko‘rinishlarining o‘z ichiga oladi:

QAH – *«Kompyuter egallash» (xaking - haking)* – kompyuter yoki tarmoqqa huquqqa ega bo‘lmasdan foydalanish. Kompyuter jinoyatining bu ko‘rinishi odatda xakerlar tomonidan begona axborot tarmog‘iga kirish uchun foydalaniladi.

QAI – *ushlab olish (interception)* – huquqqa ega bo‘lmagan holda texnik vositalar yordamida ushlab olish. Axborotni ushlab olish tashqi kommunikatsion tizim kanallari orqali yoki qo‘shimcha qurilmalar liniyalariga bevosita ulanish yo‘li orqali amalga oshiriladi.

Bunda bevosita eshitish obyektlari kabel va simli tizimlar, yer mikroto‘lqinli tizimlar, yo‘ldosh aloqa tizimlari, hamda, hukumat maxsus aloqa tizimlari hisoblanadi.

Axborotni ushlab olish va ruxsatsiz foydalanish usullarini xarakteristikasi uchun quyidagi maxsus terminologiya foydalaniladi:

– *“Qo‘ng‘iz” (bugging)* xizmat ko‘rsatuvchi personal suhbatlarini ushlab olish maqsadida kompyuterda mikrofonni o‘rnatish bilan xarakterlanadi;

– *“Ma’lumotlarni yuklab olish” (data leakage)* asosiy ma’lumotlarni, xususan, uni tizimda o‘tish texnologiyasi haqidagi ma’lumotlarni olish uchun kerakli bo‘lgan axborotni yig‘ish imkoniyati;

– *“Axlatni tozalash” (scavening)* foydalanuvchini ishidan keyin qoldirilgan ma’lumotlarni qidiruvi bilan xarakterlanadi. Bu usul ikki ko‘rinishga ega – fizik va elektron. Fizik variantda u axlat savatchalarini tekshirish va unga tashlangan izlarni, yozuvlarni va shu kabilarni yig‘ishga olib kelinishi mumkin. Elektron variant mashina xotirasida qoldirilgan ma’lumotlarni tadqiq qilishni talab etadi;

– *“Ahmoq qilish” (piggbacking)* ham muhit, ham elektron yopiq zonalarga ruxsatsiz kirish bilan xarakterlanadi. Uning mohiyati: agarda kompyuter ishi bilan bog‘liq turli predmetlarni qo‘lga olib, hamda terminal joylashgan yopiq eshik atrofida ish ko‘rinishida yursa, unda qonuniy foydalanuvchini kutib, bino eshigiga u bilan birga kirish mumkin.

– *“Dumidan ushlash” (between the line entry)* qonuniy foydalanuvchi aloqa liniyalariga ulanish mumkin bo‘lgan, hamda, oxirgi faol rejimni tugatganini anglagan holda tizimga ruxsatni amalga oshirish;

– *“Shoshilmasdan tanlash” (browsing).* Bu holda ma’lumotlar bazasiga va qonuniy foydalanuvchi fayllariga ruxsatsiz kirish tizim himoyasining zaif joylarini topish yo‘li bilan amalga oshiriladi. Qachonlardir ularni aniqlagan holda, buzg‘unchi bemalol tizimda mavjud axborotni o‘qishi va tahlillashi, uni nusxalashi, zarur bo‘lganda unga qaytib kelishi mumkin;

– *“Teshikni qidirish” (trapdoor entry)* dasturni yaratish mantig‘ida muvaffaqiyatsizlik va xatoliklardan foydalaniladi. Aniqlangan teshiklar bir necha marta ekspluatatsiya qilinishi mumkin;

– *“Lyuk” (trapdoor)* oldingisini rivojlangan holati. Topilgan “teshiklar”da dastur “buziladi”, hamda, u yerga ma’lum miqdordagi dastur komandalari qo‘yiladi. Zaruriy holda “lyuk” ochiladi, o‘rnatilgan buyruqlar esa avtomatik tarzda o‘z vazifasini bajaradi;

– *“Ko‘zbo‘yamachilik” (masquerading).* Bu holda buzg‘unchi o‘zini qonuniy foydalanuvchi ko‘rsatib, kerakli vositalardan foydalanib, kompyuter tizimlariga kirib oladi;

– *“Aldov” (spoofing)* tasodifiy holda “begona” tizimga ulanganda foydalaniladi. Buzg‘unchi ishonarli chaqiruvlarni shakllantirib, ma’lum vaqt davomida xato ulangan foydalanuvchini adashtirib, unga foydali bo‘lgan axborotni, masalan, foydalanuvchi kodlarini olishi mumkin.

Kompyuter ma’lumotlarini o‘zgartirish (QD) o‘z ichiga quyidagi jinoyat turlarini oladi:

QDL/QDT – mantiqiy bombalar (logic bomb), troyan otlari (trojan horse) – kompyuter ma’lumotlarini hech qanday huquqqa ega bo‘lmagan holda mantiqiy bombalarni yoki troyan otlarini joriy qilish yo‘li bilan.

Mantiqiy bombalar mohiyati yashirin holda qachondir, biroq ma’lum shartlarda ishga tushishi lozim bo‘lgan komandalar qatorini dasturga kiritishdan iborat.

Troyan otlari mohiyati bir vaqtning o‘zida avvalgi ishlashini saqlagan holda dastur egasi rejalashtirmagan boshqa funksiyalarni amalga oshirish imkonini beruvchi komandalarni begona dasturga yashirin holda kiritishdan iborat.

QDV – virus (virus) – kompyuter virusini kiritish yoki tarqatish yo‘li bilan kompyuter ma’lumotlarini yoki dasturlarini huquqqa ega bo‘lmagan holda o‘zgatirish.

Kompyuter virusi – turli ko‘ngilsiz harakatlarni kompyuterda bajarish uchun o‘zini boshqa dasturlarga kiritishi (ya’ni, “zararlash”), ko‘payishi va yangi viruslarni paydo qilishi mumkin bo‘lgan maxsus yozilgan dastur hisoblanadi.

QDW – ***chuvalchang*** **–** kompyuter tarmog‘ida kompyuter chuvalchangini uzatish, joriy qilish va tarqatish yo‘li bilan huquqqa ega bo‘lmagan holda kompyuter ma’lumotlarini va dasturlarini o‘zgartirish.

Kompyuter firibgarligi (QF) o‘z tarkibiga turli xildagi kompyuter jinoyatlarini sodir etish yo‘llarini oladi:

QFC – bankomatlardan naqd pullarni o‘marish bilan bog‘liq kompyuter firibgarligi.

QFF – kompyuter qalbakilashtirish – qalbaki qurilmalar yaratish yo‘li bilan kompyuter tizimlaridan o‘g‘irlash va firibgarlik.

QFG – o‘yin avtomatlari bilan bog‘liq o‘g‘irliklar va firibgarliklar.

QFM – kiritish-chiqarish dasturlarini manipulyatsiyasi – kompyuter tizimlariga noto‘g‘ri kiritish yoki chiqarish vositasida yoki dasturlarni manipulyatsiya qilish yo‘li bilan ulardan o‘g‘irlash va firibgarlik. Kompyuter jinoyatlarining bu ko‘rinishi odatda ma’lumotlarni kiritish-chiqarishda amalga oshiriladigan ma’lumot kodni (data diddling code change) almashtirish usulini o‘z ichiga oladi. Bu sodda va shu sababli ham ko‘pincha qo‘llaniladigan usuldir.

QFP – to‘lov vositalari bilan bog‘liq kompyuter firibgarliklari va o‘g‘irliklar. EHM dan foydalanilib sodir etilgan barcha jinoyatlarning

45% ini tashkil etadigan pul vositalarini o‘g‘irlash bilan bog‘liq eng ko‘p tarqalgan kompyuter jinoyatlari kiradi.

QFT - telefon firibgarligi – telefon tizimlariga xizmat ko‘rsatuvchi kompyuterlarni tadbirlari va protokollariga dahl qilish yo‘li bilan telekommunikatsion xizmatlarga ruxsat.

Kompyuter sabotaji (QS) quyidagi jinoyatning ko‘rinishlaridan tarkib topgan:

QRG/QRS – qonun bilan himoyalangan kompyuter o‘yinlarini va boshqa dasturiy ta’minotlarni noqonuniy nusxalash, tarqatish yoki e’lon qilish.

QRT –topografiya qonuni bilan himoyalangan yarim o‘tkazgichli mahsulotlarni huquqqa ega bo‘lmagan holda nusxalash – noqonuniy tarzda yarim o‘tkazgichli mahsulotlar topografiyasini nusxalash, joriy topografiyadan foydalanib, ishlab chiqilgan topografiyaga yoki yarim o‘tkazgichli mahsulotning o‘ziga huquqqa ega bo‘lmagan holda tijoriy ekspluatatsiya qilish yoki shu maqsadda import qilish.

Kompyuter sabotaji (QS) quyidagi ko‘rinishdagi jinoyatlardan tarkib topgan:

QSH – apparatli ta’minotdan foydalanib sabotaj uyushtirish: kiritish, o‘zgartirish, o‘chirish, kompyuter ma’lumotlarini yoki dasturlarini so‘ndirish; kompyuter yoki telekommunikatsion tizimlarini ishlashiga xalaqit qilish maqsadida kompyuter tizimlari ishiga aralashish.

QSS – dasturiy ta’minotga ega kompyuter sabotaji – huquqqa ega bo‘lmagan holda kompyuter ma’lumotlarini yoki dasturlarini o‘chirish, zarar yetkazish, yomonlashtirish yoki so‘ndirish.

Kompyuter jinoyatlarining boshqa ko‘rinishlariga klassifikatorda quyidagilar kiritilgan:

QZB – jinoiy faoliyatga taalluqli materiallarni saqlash, almashinish va tarqatish uchun elektron e’lonlar doskasidan foydalanish (BBS);

QZE – tijoriy sir hisoblangan axborotni o‘g‘irlash – iqtisodiy zarar yetkazish yoki noqonuniy iqtisodiy ustunlikka ega bo‘lish maqsadida u yoki bu asosga, huquqqa ega bo‘lmagan holda tijoriy sir hisoblangan axborotni uzatish yoki noqonuniy vositalar bilan o‘zlashtirish;

QZS – maxfiy xarakterdagi axborotni saqlash, almashinish, tarqatish yoki ko‘chirish uchun kompyuter tarmoqlari yoki tizimlaridan foydalanish.

2.3. Kompyuter jinoyatchilarining odatiy ko‘rinishlari

Ehtimoliy jinoyatchi baholab turib, uning AT sohasidagi bilim darajasini o‘rnatish juda muhim sanaladi. Agar shubha ostidagi shaxsning malakasi noma’lum bo‘lsa, uni yuqori deb hisoblash lozim.

Mutaxassis yoki izlanuvchi shubha ostidagi shaxs oldida AT sohasidagi malaka darajasini yashirishdan maqsadlari mos keladi. Misol keltiramiz. Tergov vaqtida mutaxassis kompyuterni ola turib, shtatli o‘chirish muolajasini yoki qo‘pol tarzda kompyuterni elektr manbaidan uzishi lozimligi masalasini yechishi kerak. Boshqa tomondan qo‘pol tarzdagi manbadan uzish natijasida unchalik muhim bo‘lmagan ma’lumotlarning bir qismi yo‘qotilishi mumkin. Biroq yaxshisi ularni saqlab qolishdir. Boshqa tomondan esa ba’zi xakerlarda (bu so‘zning yomon ma’nosida) kompyuterni o‘chirish buyrug‘i (shutdown) bilan bog‘liq ishga tushuvchi mantiqiy bombalar bilan o‘z kompyuterini qurollantirish odati ham bor. Shuning uchun ham shtatli o‘chirishda o‘z qo‘llaringiz bilan barcha dalillarni yo‘q qilish riski ham mavjud. Qaysi variantni tanlashni kompyuterning egasini malaka darajasiga qarab baholashimizga bog‘liq. Bu darajani baholashning iloji bo‘lmaganda kompyuter elektr manbasidan uzish orqali o‘chiriladi, ya’ni mantiqiy bomba mavjud deb hisoblanadi.

Bir nechta ko‘p uchraydigan kompyuter jinoyatchilarining ko‘rinishlari tavsifini keltiramiz:

1. «Xaker». Bu toifadagi buzg‘unchilarning asosiy motivatsiyasi quyidagilardan iborat: izlanuvchilik qiziqishi, qiziquvchanlik, o‘zining imkoniyatlarini isbot qilishga intilish. Kompyuter axborotini himoyalash vositalarini, ularning foydalanib bo‘lmasligini ular o‘zlarining qobiliyatlariga qarshi chaqiruvdek qabul qilishadi. Ba’zi bir izlanuvchilar bu toifadagilarning zaruriy jihati AT sohasidagi bilimlar va dasturlash deb hisoblashadi.

2. «Insayder». Kompyuter buzg‘unchisining kengroq tarqalgan toifasiga AT sohasini yaxshi bilmaydigan, lekin xizmatdagi axborot tizimiga ruxsatga ega inson kiradi. Umuman allaqachon tasdiqlanganki, kompyuter tizimlarining “buzilishi”ning katta qismi ichkaridan amalga oshiriladi. Bu haqaiatdan ham shunday. Shuning uchun ham huquqqa ega bo‘lmagan “insayder” ruxsati tergov qilishda birinchi ko‘riladigan versiya hisoblanadi. Hattoki, agarda huquqqa ega bo‘lmagan holda ruxsat tashqaridan bo‘lganda ham, uning iloji ichkaridagi xodim bilan kelishilishi evaziga amalga oshirishga mumkin bo‘lgan.

Oddiy “insayder” kompyuter jinoyatini (shaxsan yoki “tashqi” sherik bilan hamkorligi shaklida) o‘z xizmat mavqei sababli olingan ma’lumolardan foydalanilish bilan amalga oshiradi.

3. «Oq yoqa». Jinoyatchilarning bu toifasi eskidan yaxshi ma’lum bo‘lgan, biroq o‘z faoliyatlarining qurollarini kompyuterga almashtirgan g‘azna o‘g‘rilaridir. Davlatni yoki xususiy kompaniyani o‘marishning yuzlab usullari mavjud. Banal o‘g‘rilikdan tashqari bunga pora berishlar, tijoriy sotib olish, tijoriy sir hisoblangan axborotdan noqonuniy foydalanish, firibgarlikning turli ko‘rinishlari va shu kabilar. «Insayder»dan farqli bu toifadagi buzg‘unchi AT sohasida minimal malakaga ega bo‘ladi va kompyuterni jinoyatni sodir etish quroli sifatida foydalanmaydi. Kompyuter bu yerda jinoyat dalillarni, izlarni saqlovchi vazifasinigina bajaradi.

«Oq yoqa»larni sabablar bo‘yicha uch guruhga ajratish mumkin:

1) O‘z vakolatlarini suiste’mol qiluvchi xodim kompaniya yoki rahbariyatga bo‘lgan ginalari sababli. Ularni uzoq vaqt ishlagan xodimlar orasidan qidirish lozim.

2) Axloqsiz, imkoniyat tug‘ilgani sababligina o‘g‘irlik qiluvchi vijdonsiz qaroqchilar. Bu toifadagi «oq yoqa»lar uchun buzg‘unchilikning boshlangunicha lavozimda uzoq vaqt xizmat qilinmagani bilan xarakterli.

3) Og‘ir moddiy muhtojlikka, o‘g‘irlik yoki firibgarlik qilishni talab qiluvchi shaxsdan moddiy yoki boshqa bog‘liqlikka tushib qolgan zo‘ravon qaroqchilar. Bunday muammolarni atrofdagilardan yashirish qiyin – katta yutqazish, norkomaniya, oilaviy inqiroz, biznesdagi omadsizliklar. Bu guruh qaroqchilari unchalik ehtiyotkor emas, ular birinchi va ikkinchi toifadagi qaroqchilar kabi jinoyatga uzoq vaqt tayyorlanmaydi.

4. «E_tadbirkor». Bu toifadagi ehtimoliy jinoyatchi malakali AT-mutaxassisi emas va suiste’mol qilishi mumkin bo‘lgan lavozimga ham ega emas. Bu toifadagi jinoyatchilar boshidan aynan jinoiy faoliyatni rejalashtirishadi, uning noqonuniyligini juda yaxshi bilishadi. Oflayn emas, aynan kompyuter (tarmoq) muhitida huquqbuzarlik qilish qaroriga bu sohani yaxshi bilgani va kompyuterga ichki turtkisi bo‘lgani uchun emas, balki istisno tarzida ratsional tahlillash asosida keladi. «E_tadbirkor» shaxsining jihati tashkiliy qobiliyatlarning va tashabbuskorlikning borligi hisoblanadi.

5. «Ijtimoiy qarshi toifa». Yana faqatgina foyda olishga qaramaydigan internet firibgarliklari ham aniqlangan. Bundan tashqari

ularning jinoiy daromadi odatda o‘sha malakadagi mutaxassisning o‘rtacha oyligidan kam bo‘lgan. Firibgarlik qilishning sababi bunday shaxslarning jamiyatga qarshi psixopatiyasi (*sotsiopatiya*) va ularning bunday “o‘yinlarga” patologik tortishishi hisoblanadi.

Sotsiopatiya psixik tushkunlikning alohida ko‘rinishi deb tan olingan va bunday toifadagilar impulsiv harakat qilishadi hamda rejalashtirishga moyil emas, ayniqsa uzoq muddatga. Bunday tushkunlik umuman olganda odatda nafaqat kompyuter jinoyatini qilishga, balki firibgarlik qilishdan ko‘ra zo‘ravonlikka olib keladi.

2.4. Kompyuter jinoyatlarini sodir etilish yo‘llari

Jinoyatni sodir etish yo‘llari deyilganda odatda kriminalistik usullar va vositalar yordamida sodir bo‘lgan hodisa haqidagi tasavvurni, qonunbuzarning o‘ziga xos jinoiy harakatini, uning alohida shaxsiy ma’lumotlarini olish va mos holda jinoyatni fosh etish vazifasini yechishning eng optimal usullarini aniqlash imkonini beradigan turli xarakterli izlarni qoldiruvchi jinoyat sodir etilguncha, sodir etilish vaqtida hamda sodir etilgandan so‘ng subyekt axloqining obyektiv va subyektiv asostangan tizimi tushuniladi.

Kompyuter jinoyatlarini sodir etish yo‘llarini beshta asosiy guruhga sinflashtirish mumkin:

1. Kompyuter texnikasini olib qo‘yish.
2. Axborotni ushlab olish.
3. Ruxsatsiz kirish yoki foydalanish.
4. Ma’lumolar va boshqaruv buyruqlarini manipulyatsiyasi.
5. Kompleks usullar.

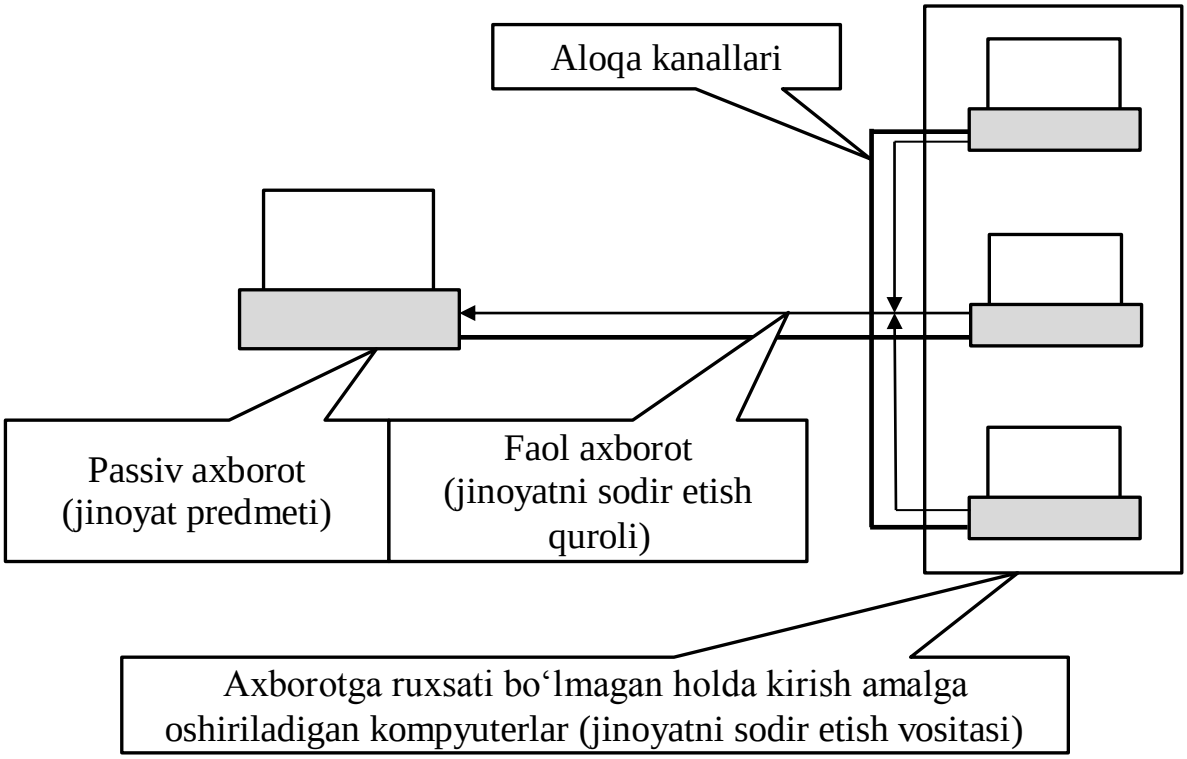
Birinchi guruhga jinoyatchining harakatlari begona mulkni o‘zlashtirishga yo‘naltirilgan jinoyatning oddiy ko‘rinishlarini sodir etishning odatiy yo‘llari kiradi. Kompyuter jinoyatining sodir etish yo‘llarining bu guruhining xarakterli farqli jihati shuki, bunda kompyuter texnikasi vositalari faqat jinoiy daxl qilish predmeti sifatida xizmat qiladi.

Ikkinchi guruhga audiovizual va elektromagnit ushlab olish usullaridan foydalanish vositasida ma’lumotlarni va mashina axborotini olishga yo‘naltirilgan jinoyat harakatiga asoslangan kompyuter jinoyatlarini sodir etish yo‘llari kiradi (5-rasm).

Faol ushlab olish (interception) kompyuterning telekommunikatsion qurilmasiga ulanish yordamida amalga oshiriladi,

masalan, aloqa kanalining telefon simi yoki printer liniyalari, yoki bevosita personal kompyuter mos porti orqali.

Passiv ushlab olish (elektromagnitli, electromagnetic pickup) ko‘plab kompyuter texnikasi vositalari, kommunikatsiya vositalari bilan birga ishlashida paydo bo‘luvchi elektromagnit nurlanishni aniqlashga asoslangan. Shunday qilib, masalan, displeyning elektron-nurli trubkasini nurlanishini 1000 m gacha masofada maxsus qurilmalar yordamida qabul qilish mumkin.



5-rasm. Faol va passiv ushlab olish

Audio ushlab olish yoki axborotni vibroakustik kanal bo‘yicha olish xavfli va yetarlicha keng tarqalgan yo‘l bo‘lib, ikki turga ega. Birinchisining mohiyati axborotni qayta ishlash vositasi apparaturasiga eshituvchi qurilmani o‘rnatishga, ikkinchisiniki esa qo‘riqlanuvchi xona doirasida injinerli-texnik konstruksiyaga mikrofon o‘rnatishdan iborat (devorlar, oyna romlari va shu kabilar).

Video ushlab olish turli videooptik texnikalardan foydalanish yo‘li bilan amalga oshiriladi.

“Axlatni tozalash” (*scavening*) axborot ushlab olishning yetarlicha original yo‘llaridan iborat. Jinoyatchilar foydalanuvchi tomonidan kompyuter texnikasi bilan ishlashdan keyin qoldirilgan

axborot jarayonining texnologik chiqindilaridan huquqqa ega bo‘lmagan holda foydalanishadi. Masalan, hattoki xotiradan va kompyuterning qattiq diskidan hamda disketalardan o‘chirilgan axborot ham maxsus dasturiy vositalar yordamida qayta tiklanishi va ruxsatsiz olinishi mumkin.

Kompyuter jinoyatlarini sodir etish yo‘llarining *uchinchi guruhiga* axborotni ruxsatsiz olishga yo‘naltirilgan jinoyatchining harakatlari kiradi. Ularga quyidagi yo‘llar taalluqli:

1. “Kompyuter abordaje” (*hacking*). Kompyuter yoki kompyuter tarmog‘iga huquqqa ega bo‘lmagan holda ruxsatsiz kirishning bu yo‘li xakerlar tomonidan begona kompyuter tarmog‘iga kirish uchun foydalaniladi.

Jinoyat odatda modem qurilmasidan foydalanilib, kompyuter tizimining abonent raqamini tasodifiy terish yo‘li bilan amalga oshiriladi. Ba’zida bu maqsadlar uchun maxsus yaratilgan parolni avtomatik qidirish dasturidan foydalaniladi. Bu dasturning algoritmi zamonaviy kompyuterlarning tezligini hisobga olgan holda harflar, raqamlar va maxsus simvollarning barcha kombinatsiyalarini terish va simvollar kombinatsiyasi mos kelgan holda ko‘rsatilgan abonentlarni avtomatik ulanishini hosil qilishdan iborat.

Oddiy terish yo‘li bilan parolni topish bo‘yicha tajribalar shuni ko‘rsatdiki, 6 simvolli parollar 6 kun uzluksiz kompyuter ishlaganda topiladi. Elementar hisob-kitob shuni ko‘rsatadiki, 7 simvolli parollarni terish uchun ingliz tili uchun 150 kundan va rus tili uchun 200 kungacha vaqt kerak bo‘ladi. Agarda harflarning registrini hisobga olinsa, bu raqamlarni 2 ga ko‘paytirish kerak bo‘ladi. Shunday qilib, oddiy terish usuli juda qiyin hisoblanadi. Shuning uchun ham oxirgi vaqtlarda jinoyatchilar tomonidan oldindan aniqlangan unga aloqador narsalarning mavzuga oid guruhlaridan kelib chiqib taklif etiluvchi parollarni terishga asoslangan “intellektual terish” usuli faol foydalanilmoqda. Bu holda *buzg‘unchi* – dasturga parol muallifi shaxsi haqidagi ba’zi joriy ma’lumotlar beriladi. Mutaxassislarning baholashi bo‘yicha bu simvollarni terish variantlarini sonini o‘n marta va shunchaga terish vaqtini ham qisqartirish imkonini beradi.

Xakerlar razvedka axborotlari va ehtimoliy raqiblarini kompyuter tarmoqlari hamda tizimlari haqidagi ma’lumotlardan yig‘ish bosqichida samaraliroq foydalanishi mumkin.

Ular allaqachon parollarni topish va fosh etish, himoya tizimlari zaif joylaridan foydalanish, qonuniy foydalanuvchilarni aldash va

kompyuter dasturiy ta’minotiga viruslarni, “troyan otlarini” va shu kabilarni kiritish bo‘yicha yetarlicha malaka to‘plashgan. Kompyuter tarmog‘i va tizimiga qonuniy foydalanuvchi ko‘rinshida kirish san’ati xakerlarga o‘z faoliyatining izlarini to‘liq o‘chirish imkoniyatini beradi, bu muvaffaqiyatli razvedka faoliyati uchun katta ahamiyat kasb etadi. Qonuniy foydalanuvchi imitatsiyasi razvedkachi-xakerga axborotning qonuniy foydalanuvchisi huquqi bilan raqib tarmog‘ida kuzatish tizimini shakllantirish imkoniyatini beradi.

2. “Axmoq qilish” (*piggybacking*). Bu yo‘l jinoyatchi tomonidan kompyuter texnikasi vositalari ishiga javobgar xodim qisqa vaqtga terminalni faol rejimda qoldirgan holda tark etgan vaqtda, kommunikatsion apparatura orqali aloqa kanaliga kompyuter terminalini ulash yo‘li bilan foydalaniladi.

3. “Qo‘lga tushurish” (*between-the-lines entry*). Bunda jinoyatchi qonuniy foydalanuvchi aloqa liniyasiga ulanadi va ish tuguganini bildiruvchi signalni kutadi, uni ushlab oladi hamda tizimga kirishni amalga oshiradi.

4. Shoshilinch bo‘lmagan tanlov (*browsing*). Jinoyatni sodir etishning bu yo‘lida jinoyatchi tizimda zaif joylarni topish yo‘li bilan kompyuter tizimiga ruxatsiz kirishni amalga oshiradi.

Bu yo‘l xakerlar orasida keng tarqalgan. Internetda va boshqa global kompyuter tarmoqlarda doimiy ravishda qidiruv, almashinuv, sotish va sotib olishlar xakerlar tomonidan buzilgan dasturlar orqali boradi. Maxsus telekonferensiyalar mavjud bo‘lib, ularda buzg‘unchi dasturlar, ularni yaratish va tarqatish muhokama qilinadi.

5. “Teshik” (*trapdoor entry*). “Shoshilinch bo‘lmagan tanlov”dan farqli kompyuter tizimi himoyasida zaif joylar qidiruvi amalga oshirilganda bu yo‘lda jinoyatchi qidiruvni konkretizatsiyasini amalga oshiradi: dastur xatoliklari yoki uni qurishdagi mantiqsizliklarga ega joylari qidiriladi. “Teshik”ni bunday aniqlanishi jinoyatchi tomonidan aniqlanmaguncha ko‘p marta foydalanilishi mumkin.

6. “Lyuk” (*trapdoor*). Bu yo‘l odingisini mantiqiy davomi hisoblanadi. Topilgan “teshik”ning joyida dastur “uziladi” va u yerga jinoyatchi tomonidan qo‘shimcha bir yoki bir nechta buyruqlar kiritiladi. Bunday “lyuk” zaruratga ko‘ra “ochiladi”, kiritilgan buyruqlar esa avtomatik tarzda bajariladi.

Kompyuter jinoyatini sodir etish yo‘llarining *to‘rtinchi guruhiga* jinoyatchining ma’lumotlarni manipulyatsiyalash usullari va kompyuter texnikasi vositasini boshqarish buyruqlaridan foydalanish bilan bog‘liq

harakatlari taalluqlidir. Bu usullar jinoyatchilar tomonidan odatda turlicha bo‘lgan huquqbuzarlik faoliyatlari uchun foydalanishi mumkin va kompyuter jinoyati bilan kurashish bo‘yicha ixtisoslashgan huquq-tartibot organlari idoralari xodimlariga yetarlicha yaxshi ma’lum.

Yo‘llarning beshinchi guruhi – kompleks usullar – kompyuter jinoyatlarini yuqorida ko‘rilgan sodir etish usullarining turli kombinatsiyalarini o‘z ichiga oladi.

Aytib o‘tish joizki, yuqori ko‘rilgan sinflashtirish aytilganidek yagona hisoblanmaydi. Xalqaro sinflashtirish bo‘yicha kompyuter tizimni ishdan chiqishiga olib keluvchi apparatli yoki dasturiy ta’minotli ***kompyuter sabotaji*** kabi yo‘llarni alohida guruhga ajratish qabul qilingan. Ahamiyatliroq kompyuter jinoyatlari dasturiy ta’minotni buzish vositasida sodir etiladi, odatda bu jinoyatni o‘zining xizmat lavozimidan, rahbariyat munosabatidan va shu kabilardan qoniqmagan ishchilar sodir etishadi.

2.5. Kompyuter jinoyatlarining turlari

Onlayn- firibgarlik. Internet-do‘kon kabi savdo-sotiqning bunday shakli bir qator sabablarga ko‘ra tadbirkorlar orasida keng qo‘llaniladi. Bu xususan, savdo-sotiq tashkillashtirishda harakatlarning kamligi bilan farqlanadi. Bek-ofisga muvofiq veb-saytlarning narhini haqiqiy savdo-sotiq maydoni tarkibi narhi bilan solishtirib bo‘lmaydi. Undan tashqari internet-do‘konlarining joriy harajatlari uning aylanmasiga bog‘liqligi, agarda proporsionalga juda yaqin bo‘lmasa, unda haqiqiy do‘kon bilan solishtirganda sezilarli darajada unga yaqin. Bu degani, agarda xaridorlarning yo‘qligida zararlar unchalik katta bo‘lmaydi. Masalan, tayyor, stabil ishlaydigan internet-do‘konning narhi 15-20 ming dollardan boshlanadi. Haqiqiy (oflayn) do‘kon bilan solishtirganda, ayniqsa katta shaharda bu shunchaki kichik puldir. Aynan internet-savdoning shu hususiyati bu yerga firibgarlarni jalb qildi. Buzg‘unchi uncha katta bo‘lmagan summani sarf qilib, normal tijoriy korxona ko‘rinishini yaratib, firibgarlik bilan yoki iste’molchilarni aldash bilan shug‘ullanishi mumkin. O‘nlab boshqa o‘ljalar to‘liq qilingan harajatlarni to‘lashadi.

Qalbaki internet-do‘konlardan tashqari firibgarlar to‘lovlarni olish uchun boshqa narsalardan ham foydalanishadi:

– xayriya, diniy tashkilotlarining, xayriya yig‘uvchi siyosiy partiyalar va harakatlarning yolg‘on saytlari;

– bechora yetimlar, urush qurbonlari, mahbuslar va shu kabilar haqidagi rahmni keltiruvchi hikoyalar ostida moddiy yordam koʻrsatish toʻgʻrisida iltimoslarga ega saytlar va spam-xabarlar;

– yolgʻon nikoh agentliklarining va alohida virtual kelinlarning saytlari;

– omonatlar boʻyicha katta foizlar vaʼda qiluvchi firibgar onlayn "banklar" va "investitsion fondlar";

– pullaringizni koʻpaytirish imkonini beruvchi toʻlov tizimlarining qora tuynuklari va zaifliklari aniqlanganligi toʻgʻrisidagi saytlar va havolalar, ularni oʻziga xos hisob raqamiga joʻnatish orqali (oʻljaning fikricha huddiki u aldoqchini aldayotgandek oʻylaydi deb hisoblanadigan asosga qurilgan firibgarlikning II tartibi ham);

– masofaviy ishni taklif qiluvchi va buning evaziga qandaydir "kirish toʻlovi" talab qiluvchi havolalar va firibgarlik saytlari.

Barcha onlayn-firibgarliklarning sxemasi quyidagicha:

– axborotni (havola) joylashtirish;

– oʻlja bilan oʻzaro aloqa qilish;

– pul oʻtkazilishini olish.

Barcha uch bosqich texnik xarakterdagi koʻrinarli izlar qoldirilishni nazarda tutadi. Firibgarlar ochiqdan-oydin oʻzlarini anonimlashtirish uchun choralar koʻrishadi. Firibgarlarni pullarni olishga nisbatan anonimlashtirishdan tashqari tezlik qutqaradi: olingan vositalarni turli toʻlov tizimlari orasida oʻtkazish yetarlicha tez amalga oshiriladi, biroq kuzatish uchun koʻp vaqt talab qilinadi.

Firibgarlar tomonidan qalbaki internet-doʻkon joylashtirilganda quyidagi koʻrinishdagi izlar aniqlanilishi mumkin:

– domen nomiga qayd maʼlumotlari; domen nomlari registratori bilan aloqa loglari; bu registratorga toʻlovlar qilish izlari;

– firibgarlarning domenini qoʻllab-quvvatlovchi DNS-serverlarini sozlashdagi izlar;

– veb-sayt joylashgan xosting-provayder bilan aloqa qilishizlari: buyurtma, toʻlov, sozlash, kontentni chiqib ketishi;

– veb-saytni reklama qilish izlari: reklama maydonlari, banner almashinish tizimlari, spam havolalar bilan aloqa;

– saytda foydalanuvchilar faolligini kuzatish izlari.

Firibgarlar aldov oʻljalari yuilag aloqa qilganda quyidagicha izlar qoldiradi:

– elektron pochta bo‘yicha, ICQ bo‘yicha, veb shakl orqali buyurtmalarni qabul qilishdagi izlar;

– potensial o‘ljalar bilan yozishuvlar izlari.

Pullarni olishda firibgarlar quyidagi izlarni qoldirishadi:

– to‘lov tizimiga pullarni kiritishdagi izlar (o‘lja ko‘rsatadigan rekvizitlar);

– firibgarliklar nazorat qiladigan hisoblar orasidagi pullarni o‘tkazishdagi izlar;

– firibgarliklarni o‘z hisoblarini masofadan boshqarish, ularni ochish va yopishdagi izlar;

– firibgarlarni vositachi bilan pullarni naqd qilish va olish bo‘yicha aloqa qilishdagi izlar.

DoS va DDoS hujumlari. DoS va DDoS hujumlari yoki “xizmatdan voz kechish” toifasidagi hujumlar huquqqa ega bo‘lmagan holda ruxsat olish ko‘rinishlaridan biri bo‘lib, aynan axboroni bloklanishiga va kompyuter tizimlari hamda tarmoqlari ishini buzilishiga olib keladi. Xuquqqa ega bo‘lmagan holda ruxsat olishning boshqa ko‘rinishlari (axborotni nusxalash, axborotni yo‘q qilish) hamda zararkunanda dasturlardan foydalanish DoS-hujumlarni amalga oshirish bosqichlari bo‘lishi mumkin.

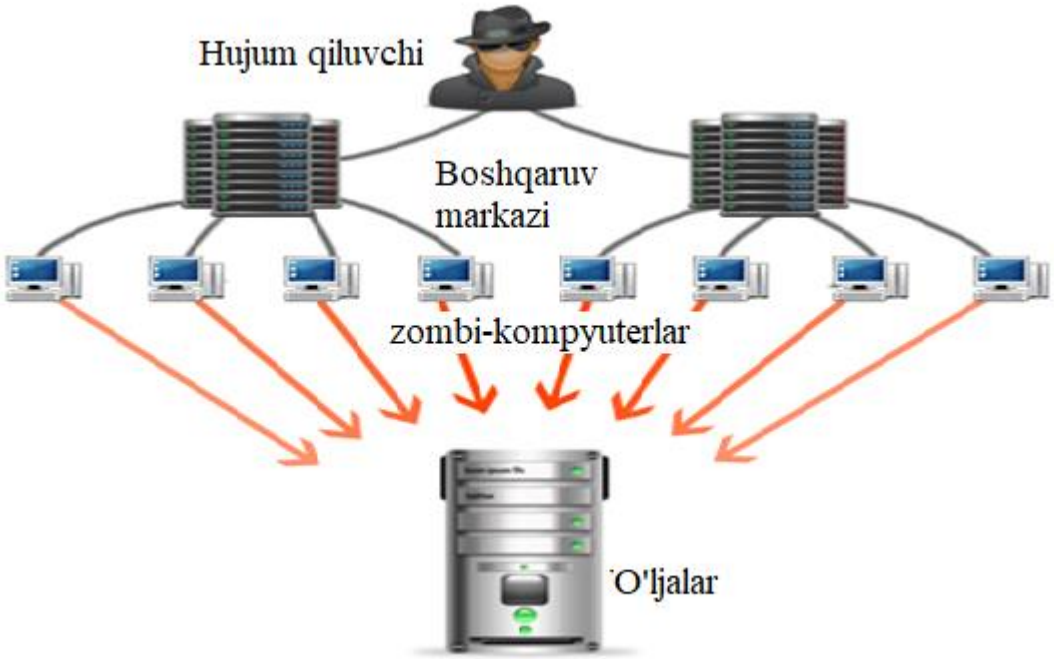
Bunday hujumlarni ikki toifaga ajratish qabul qilingan: hujum qilinayotgan tizimlarning zaifliklaridan foydalaniladigan hujumlar va zaifliklardan foydalanmaydigan hujumlar. Ikkinchi holatda hujumning o‘ziga xos “ta’sir qiluvchi faktor” hujum qilinayotgan tizimning resurslarini – protsessorni, tezkor xotirani, diskni, kanalning o‘tkazuvchanlik qobiliyatini qayta yuklash hisoblanadi.

Hozirda ham shaxsiy, ham g‘arazli DoS va DDoS hujumlari uchraydi (6-rasm).

Avvaliga shaxsiy adovatlar ustunlik qilardi. Biroq hozirda dahl qilish yoki vijdonsizlik, raqobat maqsadida g‘arazli niyatlarda DoS hujumlarining sonini o‘sish aniq tendensiyasi kuzatilmoqda.

Oddiy veb-saytga DoS-hujumini uyushtirish qiyin vazifa emas, o‘zida o‘rtacha qurollariga va aloqa kanalining o‘rtacha kengligiga ega o‘rta malakali AT-mutaxassisini qo‘lidan keladi.

Shunday qilib, DoS-hujumlari bilan bog‘liq ikki toifadagi jinoyatlarni ajratib ko‘rsatish mumkin – hujum qilinayotgan resurs egasi yoki foydalanuvchisiga ko‘ngilsizlik yaratish uchun va pul olish maqsadida.



6- rasm. DDoS hujumining arxitekturasi

Birinchi holda, bo‘hton va haqoratdagi kabi “jabrdiydani” izlash lozim. Bunda bevosita bajaruvchi o‘zi ham yoki yollangan mutaxassis ham bo‘lishi mumkin.

Ikkinchi holda, biz sovuqqon jinoiy hisob-kitob bilan duch kelamiz va jinoyat oflayn zo‘ravonlik yoki adolatsiz raqobatdan deyarli farqlanmaydi. Ehtimoliy “ye-biznesmen” jinoyatchi toifasi yuqorida “Ehtimoliy jinoyatchining shaxsi” bo‘limida tavsiflangan. Ko‘p hollarda jabrdiyda yuridik shaxs bo‘ladi.

Tijoriy tashkilotlar juda kam hollarda rasmiy tergovlarda qiziqish bildirishadi, chunki ular uchun xavfni bartaraf etish va zararlarni minimallashtirish asosiy hisoblanadi. G‘arazli niyatdagilarni jazolashdan ular o‘zlari hech qanday foyda topishmaydi. Sud jarayonida jabrdiyda rolida ishtirok etish odatda ish tajribasiga salbiy akslanadi.

DoS va DDoS hujumlarini o‘tkazishda va tayyorgarlik ko‘rishda quyidagi ko‘rinishdagi texnik xarakerdagi izlar shakllanadi:

- hujum instrumentariyalarini mavjudligi – g‘arazli niyatdagilarning kompyuterlari yoki ko‘proq bu maqsadda foydalaniluvchi begona kompyuterlarga o‘rnatilgan dasturiy vositalar (agentlar), hamda agentlarni boshqarish vositalari;
- intsrumentariyni olish, sinash, qidirish izlari;
- hujum uyushtirilgan tarmoq orqali aloqa operatorlarining loglari (ustunli trafik statistikasi);

- himoyaning texnik vositalarini loglari – trafik anomaliyalari va hujumlar detektorlari, buzib kirishlarni aniqlash tizimlari, anifludli filtrlarga ixtisoslashgan tarmoqlararo ekranlar;
- hujumni qaytarish, qarshi choralarni ishlab chiqish, insidentni tergov qilishda aloqa operatorlari texnik mutaxassislaridan maxsus olingan loglar, trafik namunalar va boshqa ma'lumotlari;
- shubhalanuvchining (hujumni buyurtmachisi) hujumni amalga oshiruvchi reklamalari, uning yozishuvlari va bajaruvchi bilan pul hisob-kitoblarini o'rganishdagi izlar;
- haqiqiylikka ishonch hosil qilish uchun hujum vaqtida hujum qilinayotgan resurslarga shubhalaniluvchi nazorat murojaatlaridagi izlar.

Tarmoq trafigidagi anomaliyalar tahlili – DDoS-hujumlarni aniqlashning yagona samarali usuli. Himoya nuqtai-nazaridan DDoS-hujumlari eng qiyin tarmoq tahdidlaridan biri hisoblanadi, shuning uchun ham samarali qarshi chora ko'rish internetga bog'liq faoliyat tashkilotlari uchun juda murakkab vazifa hisoblanadi. DDoS-hujumlar aniqlash va bartaraf etish juda qiyindir, chunki "zararli" paketlar "qonuniy" paketlardan farqlanmaydi. Tarmoqlararo ekran, "qor tuynukka" marshrutizatsiya va buzib kirishlarni aniqlash tizimlari (IDS) kabi tarmoq perimetrining xavfsizligini ta'minlash uchun odatiy texnik yechimlar va tarmoq qurilmalari tarmoq xavfsizligi umumiy strategiyasining muhim komponentlari hisoblanadi, biroq faqatgina bu qurilmalar DDoS-hujumidan to'liq himoyani ta'minlamaydi.

"Qora tuynukka" marshrutlash. "Qora tuynukka" marshrutlash jarayoni iloji boricha oldingi nuqtada maqsadli obyektga yo'naltirilgan umumiy trafikni bloklash uchun provayder xizmatlari qo'llaniladi. "Marshrutdan olingan" trafik provayder tarmog'i va boshqa mijozlarni himoyalash uchun "qora tuynukka" yo'naltiriladi. "Qora tuynukka" marshrutlashni samarali yechim deb bo'lmaydi, chunki g'arazli hujum trafikidan ishonchli paketlar ham yaroqsiz holatga keladi. Jabrdiydalar o'z trafiklaridan to'liq ayrilishadi va xaker g'alabani nishonlaydi.

DDoS-hujumlarga reaksiya. Qo'lda amalga oshiriluvchi DDoS hujumlaridan himoyalanish muolajasini "juda kam, juda kech" iborasi bilan xarakterlash mumkin. Jabrdiydani DDoS hujumiga birinchi reaksiyasi, u ulanish xizmatini ko'rsatuvchi yaqin provayderdan (bu INternet-xizmatlari-provayderi, magistral va xosting xizmatlari provayderi) manbani identifikatsiya qilishga urinadi. Agarda manzillar qalbakilashtirilgan bo'lsa yoki ular haddan ortiq ko'p bo'lsa, bu jarayon uzoq va qiyin bo'lishi mumkin va uni amalga oshirish uchun ko'plab

prvayderlarni kuchlarini birlashtirish zarur bo‘ladi. Manba identifikatsiyalansa ham bu manbaning bloklanishi barcha trafikni bloklanishiga olib keladi – yaxshisini ham, yomonini ham.

Tarmoqdagi anomaliyalar tahlili. DDoS-hujumini vaqtida aniqlash – agarda biz tarmoq resursini qulashini fakt bo‘yicha kurashishni istamak asosiy muammo shundan iborat. DDoS-hujumini aniqlashning eng samarali yo‘llari tarmoqda trafikni o‘tishi haqidagi statistik ma’lumotlarni to‘plashga asoslangan. Statistika uchun ma’lumotlar manbalari sifatida trafikni o‘zidan yoki u haqidagi ba’zi statistik axborotlardan foydalanish mumkin. Buning uchun tarmoqqa o‘rnatiluvchi qo‘shimcha sensorlar, yoki mavjud tarmoq elemenlari taqdim etishi mumkin bo‘lgan axborot foydalaniladi. Bevosita marshrutizatorlardan bunday axborot olingan taqdirda Netflow protokoli foydalaniladi. Bu protokol o‘z vaqtida marshrutizatorlar ishini optimallashtirish uchun ishlab chiqilgan, uning vazifasi agarda paket oqim talablariga mos kelsa, har bir paketni qayta ishlamasdan, uni iloji boricha tezroq qayta yo‘naltirishdan iborat. Protokol asosiy vazifani yechish uchun samarali bo‘lmadi, biroq DDoS-hujumlari bilan kurashish uchun juda qo‘l keldi va yanada kengroq tarmoq ishini tahlillash uchun ham qo‘l keldi.

Bunday qobiliyatlar protokolga dinamik rejimda o‘tgan oqimlar va paketlar bo‘yicha barcha statistik ma’lumotlar ro‘yhatga olinuvchi unga o‘rnatilgan jadvallarni shakllantirish imkoniyatini beradi: paket qayerdan kelganligi, qayerga borishi, uning protokoli, porti, qancha miqdordagi ma’lumotlar yuborilgani. Yana keyingi tahlil uchun tashqi tizimning statistik ma’lumotlarini eksport qilish imkoniyati mavjud.

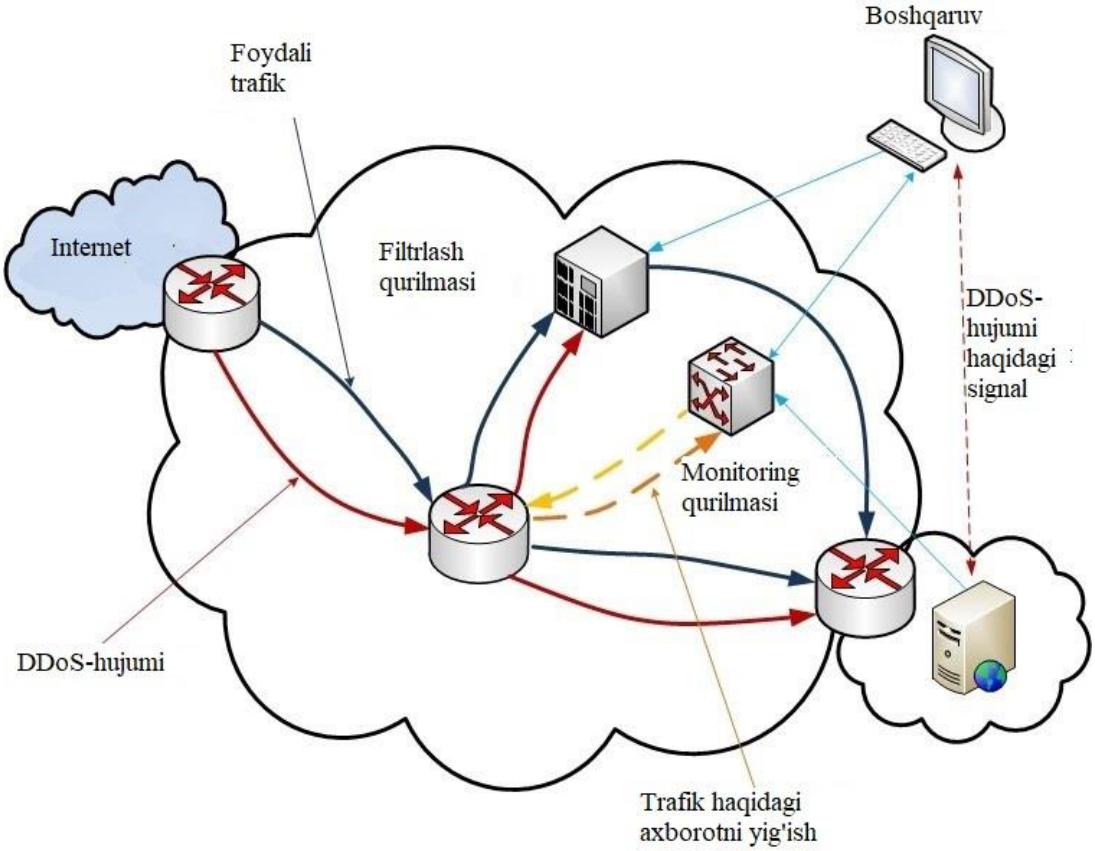
Himoyalanuvchi resursda joriy trafikning birdan normaldan farqlanish vaziyati DDoS-hujumi hisoblanadi. Aytib o‘tish joizki, tizim faqat trafikdan chetlanishnigina taniydi, u nimadan kelib chiqqanini - resurslarga qonuniy murojaatlardanmi (yangi patch qo‘yilganmi, reklama kompaniyasi o‘tkazilganmi) yoki DDoS-hujumdanmi – buni faqat resurs egasi aniqlaydi, bunday hajmli murojaatni kutganmi yoki yo‘q.

Anomaliyalar dalili aniqlangach sinflashtirish amalga oshiriladi va u qanchalik jiddiyligi aniqlanadi. Agarda DDoS-hujumi tarmoqda muammo tug‘ilishi xavfini tug‘dirmasa, unda kuzatish va hech nima qo‘llamaslik lozim, chunki resursga qonuniy foydalanuvchini qo‘ymaslik ehtimoli paydo bo‘ladi.

DDoS-hujumlariga qarshi turishning umumiy sxemasi 7-rasmda keltirilgan.

Bu yechimni texnik amalga oshirish tarmoqda ikki qo‘shimcha qurilma bo‘lishini nazarda tutadi, birinchisi kiruvchi trafik monitoringini olib boruvchi va DDoS-hujumni o‘tkazilishini aniqlaydigan, ikkinchisi esa tashqaridan keluvchi trafikni filtrlovchi (tozalovchi). Normal rejimda bu qurilmalar o‘tuvchi trafikka hech qanday ta’sir ko‘rsatmasligi kerak.

Hujum vaqtida “tozalash” qurilmasi DDoS-paketlar kabi identifikatsiyalanuvchi trafikni ushlab qoladi, bu bilan uni tor mijoz kanallariga va mijoz resurslariga nisbatan tushishiga yo‘l qo‘ymasdan, mijozga uzluksiz ravishda asosiy xizmatlarni amalga oshiradi.



7- rasm. DDoS-hujumlarga qarshi chora ko‘rish sxemasi

Zararkunanda dasturlar.

Antivirus analitiklari zararkunanda DT tijoratlashuviga yaqqol tendensiyani aytishmoqda. Hali 10-15 yil oldin deyali barcha viruslar va chervlar aniq g‘arazli maqsad bezorilik yoki qiziqish uchun yaratilgan.

Zamonaviy zararkunanda dasturlar orasida ko‘pchiligini foyda olish maqsadidagi dasturlar tashkil etadi. Ularning asosiy turlari (maqsadi nuqtai-nazaridan) quyidagilar:

– Zombi-tarmoqlarni yaratish uchun **troyan dasturlari,** keyin ular spam tarqatish, DoS-hujum, fisher saytlarini tashkil qilish va shu kabilar uchun foydalaniladi; odatda ular o‘zini-o‘zi tarqatish mexanizmiga ega bo‘ladi;

– **Spyware,** ya’ni shaxsiy ma’lumotlarni – to‘lov tizimlari parol va kalitlari, bank kartalari rekvizitlari va firibgarlik yoki o‘g‘irlik uchun foydalanish mumkin bo‘lgan boshqa ma’lumotlarni o‘g‘irlash uchun troyanlar va chervlar;

– **Adware,** ya’ni shaxsiy kompyuterga yashirin kirib oluvchi va foydalanuvchiga ruxsatsiz reklamalarni ko‘rsatuvchi zararkunanda dasturlar (ba’zida adware sinfiga zararkunanda dasturlargina emas, “qonuniy” bo‘lgan foydalanuvchi ruxsati bilan reklama ko‘rsatuvchi dasturlarni ham kiritishadi);

– Foydalanuvchi imtiyozlarini oshirish uchun xizmat qiluvchi va “buzilgan” kompyuter harakatlarini yopish uchun xizmat qiladigan **rutkitlar;**

– Belgilangan vaqtda yoki ma’lum shartlar bajarilishida kompyuterdagi barcha sezgir axborotni avtomatik yo‘q qilish uchun mo‘ljallangan **mantiqiy bombalar;**

– **“ransomware”** – o‘lja kompyuteriga yashirin tarzda troyan dasturi ko‘rinishi ostida kirib olgach foydalanuvchi axborotdan iborat fayllarni shifrlaydi, so‘ngra foydalanuvchi fayllarini qayta tiklash imkoniyati uchun pul to‘lashni talab qiladi.

Zamonaviy zararkunanda dastur jinoiy biznes uchun texnologik element vositasi bo‘lgani kabi, zamonaviy virus yozuvchi ham o‘z-o‘zidan ishlamasdan boshqalarni buyurmasini bajaradi. Bu buyurtma ***virmeyker-dasturchi*** texnik vazifani olib, uni bajarib, tayyor mahsulotni buyurmachiga berganda to‘g‘ridan-to‘g‘ri buyurtma bo‘lishi mumkin. Bu buyurtma virmeyker qora bozor ehtiyojlarini bilgan holda o‘z mahsulotlari bilan uni qoniqtirishga urinadi, keyinchalik esa mustaqil amalga oshirganda (foydalanuvchilarga litsenziya beradi) to‘g‘ridan-to‘g‘ri bo‘lmagan buyurtma ham bo‘lishi mumkin.

Uzoq vaqtdan beri butun jinoiy g‘oyani – zararkunanda kod yozishni, uni qo‘llashni, qo‘llash natijasini foyda olish uchun ishlatishni yagona bir kishi amalga oshirgan hol uchramagan.

Shunday qilib, zararunanda dasturni ***yaratuvchisi*** – bu deyarli har doim jinoiy guruh a’zosidir. Uning faoliyati buyurtmachilar va

zararkunanda dasturlar foydalanuvchilardan ayri holda ahamiyatga ega emas.

Zararkunanda dasturlarni yaratishdan tashqari ularni qo‘llash ham jinoyatdir. Bunday dasturdan foydalanuvchi shaxs ham ko‘p hollarda o‘z mehnatining natijalarini bevosita bajarmasdan, jinoiy guruhning boshqa a’zolariga sotadi yoki beradi.

Va nihoyat uchinchi toifa – bu zararkunanda dasturlarni qo‘llash natijalarini ***amalga oshiruvchilar***, ya’ni **spamerlar, firibgarlar, karderlar, talonchilar**.

Jinoiy “jamoalarga” misollar keltiramiz.

Spammerlar. Birinchi xabar tarqatuvchi foydalanuvchi kompyuteriga yashirin tarzda kiritish uchun DT ni yaratadi va uni rivojlantiradi (troyanlar). Ikkinchi kishi birinchisidan ko‘rsatilgan dasturdan foydalanish huquqini sotib olib, uni massali tarzda tarqatadi, signallarni qabul qiladi va muvaffaqiyatli kiritilgan troyanlarni hisobga oladi, ularni tuzilmaga ega zombi-tarmoqlarga birlashtiradi. Tayyor tarmoqni (butunligicha yoki qisman, doimiy va ma’lum vaqtga) u uchinchi shaxsga sotadi, u esa uning yordamida spam havolani yuborishni amalga oshiradi. O‘sha spam yordamida buyurtmachilarni qidiradigan to‘rtinchi xabar tarqatuvchi havolalar yuborishga buyurtmalarni qabul qiladi, buyurtmachidan olingan pullarning bir qismini uchinchi shaxsga xizmat haqi sifatida o‘tkazadi. Beshinchi shaxs maqola uchun elektron pochtalar manzillarini verifikatsiya qilish va yig‘ish bilan shug‘ullanadi. Yig‘ilgan manzillar bazasini (yoki bunday bazalarga yozilishni) to‘rtinchi shaxsga yoki uchinchi shaxsga sotadi.

Karderlar. Birinchi xabar tarqatuvchi bank kartalarini atributlarini *yig‘ish* bilan shug‘ullanadi. U sotuvchi yoki ofitsiant bo‘lib, sezdirmasdan mijoz kartalaridan ma’lumotlarni olishi mumkin. U firma yoki bank menejeri bo‘lishi mumkin va xizmat lavozimidan foydalanib, kartadar ma’lumotlar bazasiga ruxsat olishi mumkin. U zararkunanda dasturlar josuslarni (spyware) kiritib yoki fishing orqali karta raqamlarini olishi mumkin. Ma’lum miqdordagi bank kartalariga ega bo‘lingach, birinchi xabar tarqatuvchi ularni ikkinchiga yuboradi. Ikkinchi shaxs jinoiy biznes *tashkillashtiruvchisi* rolini o‘ynaydi.

U o‘zida ma’lumotlarni jonlantiradi va bajaruvchilarga taqsimlaydi. Uchinchi tarqatuvchi ikkinchining buyurtmalari bo‘yicha karta rekvizitlarini verifikatsiyasini *bajaradi*, ya’ni ularni haqiqiyligini va to‘lovga yaroqliligini tekshiradi. To‘rtinchi tarqatuvchi pulli veb-saytni yoki qalbaki-do‘konni yoki karta orqali xizmatlar to‘lovini

amalga oshirish imkoniyatiga ega internet-kazinolarni *yaratadi* va qo‘llab-quvvatlaydi. U billing kompaniyalari bilan bir nechta shartnomaga ega va vaqti-vaqti bilan ularni hamda o‘zining e’lonlarini o‘zgartirib turadi. Bu pullarni qonuniylashtirish uchun mexanizmdir. Beshinchi guruh – *siquvchilar* deb ataladi. Ular ikkinchi shaxsdan o‘nlab bank karta raqamlarini partiyalarni olishadi va turli mijozlar ko‘rinishadi to‘rtinchi shaxsning qonuniy pullarni naqd qiluchi korxona orqali kiriishadi. Bunda ular texnik vositalar yordamida turli davlatlardan va turli kompyuterlardan ruxsatni emulyatsiyalashlari lozim. Ular ishlari uchun to‘langan haqni olishadi, kamdan kam hollarda – foydadan foiz olishadi. Oltinchi shaxs amalga oshirishni boshqa kanalidir, u narsalar *kardingi* bilan shug‘ullanadi. Ikkinchidan “tanlab olingan” eng istiqbolli kredit raqamlarni olib, ulardan haqiqiy internet-do‘konlarda xaridlar qilish uchun foydalanishadi. Asosan qimmat, og‘ir bo‘lmagan va yaroqli texnikalar – mobil telefonlar, videokameralar, kompyuter to‘plamlari va shu kabilar xarid qilinadi.

Tabiiyki, ular uning manziliga buyurtma berishmaydi. Buyurtmalar qabul qilish uchun yettinchi sheriklar guruhi – *drop* mavjud. Ular boy mamlakatlardan kelgan fuqarolardir, chunki onlayn-do‘konlarning aksariyati AQSH, Kanada va Yevropa Ittifoqi hududlaridan tashqarida buyurtma bermaydi, va agar qilsalar, bu xaridorlarni juda ehtiyotkorlik bilan nazorat qiladilar. Droplarning ishi do‘kon xodimini buyurtma bergan telefonni tasdiqlash, qabul qilish va darhol oltinchi ishtirokchiga (ba’zan izlarni mustahkamlash uchun boshqa dropga) jo‘natishdir. Droplar talabalar kabi jamiyatning kam daromadli qatlamlari tomonidan to‘planadi, odatda bir drop bir necha hafta oralig‘ida faqat o‘nlab operatsiyani amalga oshiradi. U to‘lovni tovarlarning qiymatini bir qismiga yoki foiziga ko‘ra oladi. Nihoyat, sakkizinchi yordamchi paketlarni dropdan qabul qilish va sotish bilan shug‘ullanadi.

Fisherlar. Birinchi hamkor banklar va boshqa muassasalarning veb-saytlarini joylashtirish bilan shug‘ullanadi. Bunday saytlarning dasturlari mijozning maxfiy ma’lumotini zudlik bilan shubhali shaxslarga jo‘natish uchun tizim bo‘lib, u tabiiy ravishda buni seydirmaslik maqsadida to‘g‘ridan-to‘g‘ri bajarmaydi. Ikkinchi hamkor bu saytlarni joylashtiradi, noto‘g‘ri xatlar qiladi va ularni yuboradi, lekin mustaqil ravishda emas, balki buning uchun spammerlarning xizmatlaridan foydalanadi. Uchinchi sheriklar ma’lumotlarni karterlarga (pulli kodlar yoki to‘lov tizimlariga parollar) yoki boshqa jinoiy

tuzilmalarga amalga oshirish bilan shug‘ullanadi. Jinoiy guruh pin kodlarini mustaqil ravishda amalga oshirish bilan shug‘ullanadi. Undan keyin "plastik", ya’ni do‘konlar va bankomatlar uchun bank kartalarining nusxalarini ishlab chiqaruvchi to‘rtinchi sherik, shuningdek, bankomatlardan pulni tortib oladigan, karta va pin kodlariga ega beshinchi guruh ishga kirishadi.

Ko‘rib turganimizdek, zararli dastur har qanday holatda ham katta jinoyat maqsadlaridan biri uchun vosita rolini o‘ynaydi. Ham yaratuvchisi, ham zararli dastur ilovasi ham umumiy rejani amalga oshiradi.

Shunday qilib, zararli dasturlarni yaratish va ulardan foydalanish bilan bog‘liq holatlarda, ehtimol, jinoyatchi guruhlar ushbu guruhda ishlaydigan yoki daromadlar foizi yoki jinoyat qurollarini mustaqil yaratuvchi sifatida ishlaydigan jinoiy guruhning a’zosi hisoblanadi. YA’ni, iqtisod nuqtai nazaridan, virus yozuvchisi ba’zi hollarda o‘z mehnat kuchini, ba’zilarida mehnatini, uchinchisida esa uning shaxsiy mahsulotini sotadi.

Odatda bu kasbni tanlagan, jinoyat yo‘liga kirgan professional dasturchidir. Uning maqsadi puldir.

Xakerlik faoliyatiga olib kelgan sabablar, ya’ni o‘zini o‘zi tasdiqlash va tadqiqot qiziqishlari faqat birinchi bosqichda, u jinoiy faoliyat bilan shug‘ullanganda muhim ahamiyatga ega. Moddiy foyda maqsadi hamisha asosiy hisoblanadi.

Dialer (dialers). To‘g‘ridan-to‘g‘ri pullik telefon liniyalaridan adolatsiz foydalanish - bu firibgarlikning bir turi. Chaqirayotgan abonentning "suhbat" uchun katta miqdorda haq to‘lashi bilan mos raqamni yozgan holda, firibgarlar abonentlar tomonidan qo‘ng‘iroqlarni amalga oshirish uchun har qanday usulda harakat qilishmoqda. Ular ushbu raqamni bilvosita noto‘g‘ri reklama qilish, SMS jo‘natish va ushbu raqamdan chiquvchi qo‘ng‘iroqlarni amalga oshirish uchun abonentga qayta qo‘ng‘iroq qilish, o‘z raqamiga qo‘ng‘iroq qilish, operator billing tizimining kamchiliklarini ishlatib, telefon tarmog‘iga qo‘ng‘iroqlar haqida noto‘g‘ri ma’lumot kiritish, foydalanuvchining modemlarini qo‘ng‘iroq qilishni taqiqlashga qodir zararli dasturlardir.

Shartnoma shartlariga ko‘ra, qo‘ng‘iroq qiluvchi operator qo‘ng‘iroqni qabul qiluvchi abonentning operatoriga qo‘ng‘iroq qiladi va undan so‘ng uning abonentidan pul olishga harakat qiladi.

Biz batafsil bunday firibgarlik eng keng tarqalgan turlaridan biri-qo‘ng‘iroq qilgich-dasturlar (dialer) yordamida amalga oshiriluvchi firibgarlikni tasvirlab beramiz.

Biroq bugungi kunda sudlar zararli dasturlarni stixiyali kuch, ularning harakatlarini esa noqulaylik tug‘diruvchi vaziyatlar sifatida tan olmaydilar va shuning uchun bunday dasturlardanjabrlangan foydalanuvchilar hali ham qo‘ng‘iroqlar uchun haq to‘lashlari kerak. Biroq ba’zida telekommunikatsiya operatori bunday abonentning qarzini qonunga ko‘ra emas, balki adolatga ko‘ra "kechirish" ga moyil.

Zararli dasturiy ta’minotni ishlab chiqarishda quyidagi raqamli izlar mavjud:

– zararli dasturning dastlabki kodi, uning oraliq versiyalari, virmaker kod bo‘laklaridan qarzdor bo‘lgan boshqa zararli yoki ikkilamchi dasturlarning manba kodi;

– zararli dasturiy ta’minotni yaratuvchisi o‘z-o‘zida sinab ko‘rgan turli xil ishlab chiqaruvchilarning virusga qarshi dasturiy ta’minoti, shuningdek xatolarni tog‘irlash va disassemblashtirish vositalari;

– zararli dasturlarni boshqarish uchun dasturiy ta’minot (ularning aksariyati "mijoz-server" sxemasiga muvofiq ishlaydi, bir qismi qurbonning kompyuteriga o‘rnatilgan, qolgan qismi esa tajovuzkorning to‘g‘ridan-to‘g‘ri nazorati ostida ishlaydi);

– operatsion tizimning turli xil versiyalari bo‘yicha zararli dasturlarni tekshirish vositalari va izlari;

– zararli dasturning mijozlar yoki foydalanuvchilar bilan aloqa izlari, ularning nusxalarini va hujjatlarni topshirish, to‘lash.

Zararli dasturlarni tarqatishda va ishlatishda quyidagi raqamli izlar mavjud:

– turli OT versiyalari bo‘yicha zararli dasturlarni tekshirish usullari va izlari;

– zararli dasturni yaratuvchisi yoki distributori bilan aloqa qilish;

– zararli dasturni boshqarish uchun dasturiy ta’minot, ushbu dasturni jabrlanuvchiga kiritish to‘g‘risidagi ma’lumotlar, faoliyat natijalari (parollar, tayyorlik hisobotlari, o‘g‘irlangan shaxsiy ma’lumotlar);

– zararli dasturlarni tarqatish vositalarini yoki uni tarqatish uchun buyurtma berganlar bilan aloqalarni ta’minlash.

Antivirus logi, shuningdek, tekshiruv davomida tekshirilayotgan zararli dasturlarning izlari, ekspertga garchi ushbu dasturning bajarilayotgan kodi topilmasa ham tekshirilayotgan kompyuterda muayyan zararli dasturiy ta’minot o‘rnatilganligini qat’iyan ta’kidlash imkonini beradi. Bunday tajribani tegishli antivirus dasturlarini ishlab chiqaradigan yoki saqlaydigan tashkilotga topshirish muqobilroqdir.

Defeys. Ushbu jinoyat shundan iboratki, buzg‘unchilarning bir yoki bir nechtasi jabrlanuvchining ommaviy veb-saytining ko‘rinishini, ko‘pincha uning nomi o‘zgartiradi. Texnik jihatdan, bu veb-server ma’lumotlari saqlanadigan katalogga yozish uchun ruxsatni olish yo‘li bilan amalga oshirilishi mumkin. Bundan tashqari, ko‘pincha veb-serverning o‘zi yoki uning CGI-skriptlaridan biridagi zaiflikdan foydalaniladi. Shubhasiz, tajovuzkor qonuniy foydalanuvchilardan biri hisobiga muntazam funksiyadan foydalangan holda veb-sahifani o‘zgartiradi, chastotani kamaytirish uchun sabablar quyidagilardan iborat:

– ularning malakalarini oshkora ko‘rsatish istagi;

– siyosiy, diniy va boshqa g‘oyaviy sabablar;

– jabrlanuvchi yoki uning biron bir xodimidan biriga shaxsiy adovat

– veb-sayt egasini obro‘sini to‘kish, raqobat qilish uchun uning biznes obro‘sini buzish, birjada spekulyasiyalash maqsadida uning kapitallashuviga ta’sir ko‘rsatish;

– dasturiy ta’minotdagi zaifliklarning mavjudligini namoyish etish, unga e’tiborni jalb qilish istagi.

Ehtimol, jinoyatchi «xaker» modeliga yoki kamroq hollarda «insayder» modelga mos keladi. Tajovuzga uchragan kompyuterda ko‘plab izlar qolmaydi, agar imkon bo‘lsa, haker ularni buzishga harakat qiladi. Xaker hujum qilingan veb-saytni tekshirish va unga kirish uchun qidiruv tugunlari sifatida foydalanadigan kompyuterlarda qo‘shimcha izlar mavjud. Bundan tashqari foydali statistika ma’lumotlar tranzit provayderlari ham foyda beradi. Qo‘shimchasiga mehmonning shaxsiy kompyuterida, yana ko‘plab izlar - qayta ishlangan yoki yangi yaratilgan veb-sahifani va oraliq versiyalari, maqsadli veb-sayt va oraliq tugunlardagi zaifliklarni topish va ishlatish vositalarini ruxsatsiz foydalanishni amalga oshirish vositalari bo‘lishi kerak.

Aks holda, aksiya aks ettirilmasligi mumkin - o‘zgartirilgan saytlar uzoq vaqt davomida bunday holatda qolmaydi, odatda egasi odatiy

koʻrinishni tezda tiklaydi, shuning uchun, tajovuzkor "buzish"dan soʻng darhol yoki undan avval biron bir tarzda dunyoga uning jinoyati haqida xabar beradi. Bunga misol tariqasida elektron pochta, yangiliklar guruhi maqolasi yoki veb-forumni keltirish mumkin. Bularning barchasi qoʻshimcha izlarni qoldiradi.

Shuningdek, tajovuzkor muntazam defeys natijalarini tekshiradi va jamoatchilikning unga munosabatini kuzatadi. U bu xatti-harakatlarni shaxsiy kompyuterdan anonimlashtirish uchun maxsus choralarsiz amalga oshirishi mumkin.

Koʻpincha jabrlanuvchi yuridik shaxsdir. Odatda, jabrlangan kompaniya hodisa haqidagi maʼlumotlarni oshkor qilishdan manfaatdor emas. Agar xabarning keng yoyilishi oldindan roʻy bergan boʻlsa, jabrlanuvchining holati oʻzgarishi mumkin, chunki ishbilarmonlik obroʻsiga zarar yetkazilishini kompetsatsiyalash, aksiyadorlarga va mijozlarga sabablarni tushuntirishga toʻgʻri keladi. Tezkorlik bilan tajovuzkorni topib, adolatni taʼminlash, obroʻ va jamoatchilik bilan munosabatlar nuqtai nazaridan kichik tovondir.

Karderlik. Bank kartalari sohasida soxta bozor juda katta. Buni quyidagicha baholash mumkin. Har bir bankning karta operatsiyalari uchun maʼqul boʻlgan zarar limiti mavjud. U 0.1-0.5% oraligʻida boʻladi. Bu karta operatsiyalari umumiy aylanmasining kamida 0,1% karterlarga toʻgʻri keladi degan maʼnoni anglatadi.

Bank (toʻlov) kartalari bilan bir necha turdagi firibgarlik mavjud. Ularning barchasi bitta sxemaga kiritilishi mumkin:

< **qabul qilish - tarqatish – amalga oshirish** >

Birinchi bosqichda bank kartalari boʻyicha maʼlumotlar turli yoʻllar bilan olinadi. Ikkinchi bosqichda ular turlanadi, nazorat qilinadi, tasniflanadi va ulgurji vositachilar (chakana narhda sotib olish, ommaviy sotish, chakana narhda sotish) orqali sotilishi mumkin. Uchinchi bosqichda bank kartalari maʼlumotlari amalga oshiriladi, yaʼni pulga aylantiriladi.

Koʻrsatilgan zanjir hech qachon bir kishi tomonidan bajarilmaydi. Bosqichlarning har biri oʻzining oʻziga xos koʻnikmalariga, tegishli sohada tajribaga, rasmiy lavozimga, texnologiyani ishlata olishga bogʻliq. Shuning uchun jinoyat zanjiri har doim kamida uchta sherikni oʻz ichiga oladi.

Qiymatli bank kartasi maʼlumotlar toʻplamlari:

(1) raqam, amal qilish muddati, egasining nomi, cvv yoki cvc kodi;

(2) toʻldirish kartasi;

(3) qoldiq + pin-kod.

Uchinchi variant - karderlar uchun eng jozibalisidir. Ushbu ma’lumotlar to‘plami eng tezkor tarzda naqd pulga aylanishi mumkin va ayni paytda maksimal miqdorni olishi mumkin.

Bank kartasi ma’lumotlarini olish usullari (8-rasm):

8- rasm. To‘lov joylarida karta dampini yashirin tarzda olish uchun firibgarlar tomonidan ishlatiladigan portativ hisoblagichlar

- bunday ma’lumotlarning saqlanadigan yoki ishlov beriladigan serverga, masalan, do‘kon yoki bank serveriga masofadan ruxsatsiz kirish huquqi - ko‘pincha bilmagan odamlar tomonidan qabul qilingan, lekin amalda kamdan-kam uchraydigan usul;
- o‘zlarining rasmiy amalidan va kompaniyaning axborotni muhofaza qilish tizimidagi nuqsonlardan foydalangan holda bunday ma’lumotlardan foydalanish - ko‘pincha maxfiy axborot egalari tashqi tahdidlardan himoyalanish uchun ortiqcha chora-tadbirlar ko‘radi, ammo ichki tahdidlardan himoyalanishni e’tiborsiz qoldiradi;
- (kamdan-kam) internet-trafikni ushlab turish, karta ma’lumotlari aniq matnda (HTTP yoki elektron pochta orqali) uzatish;
- bank plastik kartochkalaridan ma’lumot olish yoki xaridorlarni savdo va umumiy ovqatlanish korxonalarida xizmat ko‘rsatish vaqtida olib tashlash usullari oldingi usulga o‘xshash, biroq uning xususiyati kartochkadan bevosita aloqa qilish vaqtida ma’lumotdan to‘g‘ridan-to‘g‘ri ko‘chirilishidadir;
- fishing usulidan foydalangan holda karta ma’lumotlarini yoki pin kodlarni qo‘lga kiritish;

- soxta bankomat (ATM) yoki ATM qo‘shimchalari yordamida damp va pin kodlarni olish (scimming);
- kartani firibgarlik yo‘li bilan olish ("Livan o‘rami" va boshqalar);
- kartalarni egasidan odatdagi holda o‘g‘irlash (ko‘pincha pin kod pul sumkasida joylashgan qog‘ozga yozilgan bo‘ladi).

Quyida ushbu bank kartalarini sotib olish va sotishning yuqorida ko‘rsatilgan usullarini batafsilroq tushuntirilgan.

Skimming (skimming). Karderlar uchun eng foydali chiziq - kartaning magnit chizig‘ining to‘liq nusxasi (dampi) va uning pin kodi. Bunday ma’lumotlar sizning hisobingizdan mablag‘ qoldig‘ini hamda barcha kredit limitini olish imkonini beradi. Odatda bu o‘n minglab dollar deganidir. Bunday jekpot kartalari uchun karderlar juda ko‘p narsalarga tayyordirlar. Hatto bankirlar, mijoz raqamini bilib olgach, karderga xabar berish va birgalikda hamkorlik qilishdan doim ham tiyila olmaydilar. 1990 yildagi soxta bankomatlar va terminallar o‘rnatish mashhur edi (9-rasm)

Ushbu qurilmadan foydalangan holda, karderlar foydalanuvchining kartasidagi magnit liniyadan nusxa olishgan va keyinchalik hisobidan mablag‘ni yechib olishgan.

Ularning aksariyati hatto mijozlarga pul yoki mol-mulk ham bergan. Bugungi kunda bunday bankomatlar kamroq uchraydi.

9- rasm. Bankomatning soxta birikmasi

Odatiy bankomatlarga "qo‘shimchalar" ham tez-tez uchrab turadi, bu mijoz tomonidan sezilmagan holda magnit chiziqdan ma’lumotlarni o‘qiydi va kiritilgan PIN-kodni "ko‘rib oladi" (10, 11-rasm) .

10- rasm. Reklama ostiga yashiringan va mijozning pin-kodini suratga oluvchi videokamera

11- rasm. Kiritilayotgan pin-kodni qabul qiluvchi klaviatura qo‘shimchasi

Ushbu usulning tarqalishi kartochkalarni ishlab chiqaruvchilar hozirda kartani o‘quvchi uchun kartani tortib olinmaydigan mexanizmni taqdim etishi bilan izohlanadi. Kartochka bankomatga tortiladi va magnit chiziqni mumkin bo‘lgan ayg‘oqchi qurilmalar tomonidan o‘qish uchun qiyinlashtirish uchun bir necha tortilishda mashinadan olinadi. Biroq bunga qarshi texnik chora-tadbirlari allaqachon kashf qilingan.

Real plastik. Karderlar jargonida "real plastik" bank kartalarining to‘liq nusxalari demakdir. Ular rangli tasvirga ega bo‘lishi, gologramma,

foydalanuvchining embossirlangan (o‘yilgan) nomi va kerakli ma’lumotlarni o‘z ichiga olgan magnit chiziq bo‘lishi kerak.

Ushbu amaliyot usuli damp karta talab qiladi. PIN-kod talab qilinmaydi. Kartaning qattiq nusxasi dampga asoslanib amalga oshiriladi. Bu nafaqat magnit chiziqdagi to‘g‘ri ma’lumotga ega bo‘lishi, balki shunga o‘xshashi ham kerak. Kartada chizilgan rasm, albatta, asl nusxaga to‘g‘ri kelishi shart emas, lekin u bo‘lishi va yuqori sifatli amalga oshirilishi kerak: bulg‘anganmasligi, bo‘linmasligi lozim. Bank va kartaning nomi kodga mos kelishi (karta raqamining dastlabki 6 raqami) ham muhim; Biroq sotuvchilar kamdan-kam hollarda bunga e’tibor berishadi.

Oq plastik. Faqat saqlangan magnit chiziqlarga ega bo‘lgan kartaga karterlar uchun "oq plastik" deb nom beriladi. Uni ishlab chiqarish juda arzon. Biroq foydalanish maydoni faqat bankomat bilan cheklangan. Albatta, PIN-kodni bilish kerak.

Qora bozorda damp kartochkalarning bir nechta to‘plami + PIN-kodlar qimmat turadi, ammo u bankomatdan barcha balans va kredit limitini olib tashlash orqali kartochka hisobini quruqlashtirish uchun ishlatilishi mumkin. Ko‘pgina banklar bankomat bitimlariga cheklovlar qo‘yadi - geografiya bo‘yicha, bir vaqtning o‘zida maksimal miqdorda pul yechishga, kunlik maksimal miqdor. Bu karderlar faoliyatini qiyinlashtiradi. Pullar yechib olinmaguncha karta to‘xtatilishi va to‘xtatish ro‘yxatiga qo‘shilishi mumkin.

Trafik bilan firibgarlik. Aloqa operatorlari uchun avtomatlashtirilgan hisoblash tizimlari (billing tizimlari), shuningdek, ma’lumotlarni yig‘ish vositasi bunday tizimlar uchun (prebinding, mediaton) har doim firibgarlar, o‘g‘rilar va boshqa jinoiy shaxsning qiziqish doirasida bo‘ladi. Billing tizimidagi ma’lumotlarni o‘zgartirib, siz katta miqdordagi firibgarlik, o‘g‘irlik, talonchilikni amalga oshirishingiz mumkin. Bunday tizimlarning murakkabligi juda katta, xodimlarning ko‘pchiligi va korxonaning mijozlari bir vaqtning o‘zida ularga kirish imkoniga ega, shuning uchun ma’lumotlarni olish va o‘zgartirish uchun har doim yetarli texnik qobiliyat mavjud.

Billing ma’lumotlarining ayyorligi juda keng tarqalgan. Bu shunchalik keng tarqalganki, bu kabi huquqbuzarlik uchun mablag‘larni hisobga olishning standartlari mavjud. Bozorda bunday operatsiyalarni aniqlash va oldini olish uchun maxsus dasturiy mahsulotlar mavjud bo‘lib, ular "fraud management systems" deb ataladi. Nomning o‘zi, bu firibgarlikning oldini olish emas, balki bunday firibgarlikdan kelib chiqadigan zararning kamayishi haqidaligini bildiradi.

Bunday jinoyatlarni tergov qilish ikki sohada maxsus bilimlarni talab qiladi. Birinchidan, biznes kommunikatsiyalari sohasida. Trafikni uzatish tartibi, uning texnik tashkil etilishi, operatorlar o‘rtasidagi o‘zaro hisob-kitoblar, tarif xususiyatlari - bularning hammasi maxsus bilim sohasi hisoblanadi. Ikkinchidan, IT bilimi talab qilinadi, chunki barcha billing tizimlari kompyuter axborot tizimlari bo‘lib, ularga ruxsatsiz kirishni tashkil etish tegishli maxsus bilimlar mavzusidir.

Fishing (phishing) - qurbonlarning ijtimoiy injineriya usullari bilan maxfiy ma’lumotlarini olish. Odatda, bank kartasi raqamlari, ularning PIN-kodlari, parollarni bank hisobini boshqarish tizimiga (onlayn-banking) va undan keyin pulga aylanishi mumkin bo‘lgan boshqa ma’lumotlardan bahs yuritiladi. Eng ko‘p uchraydigan banklar va to‘lov tizimlari – “Citi bank”, “eBay” va “PayPal”.

Ishonchli ma’lumotlarni qo‘lga kiritish soxta elektron pochta xabarlari va/yoki soxta veb-saytlar orqali sodir bo‘ladi. Odatda, ular firibgar tomonidan taklif qilingan protseduraga rioya qilmasa, masalan, foydalanuvchi hisobini yopish yoki xizmat ko‘rsatishni to‘xtatib qo‘yish bilan qo‘rqitishga harakat qilishadi. Ko‘p hollarda, har doim ham bo‘lmasada, da’vo qilingan voqea-hodisa autentifikatsiya ma’lumotlarini yo‘qotish, boshqa favqulodda holatlar, hatto firibgarlarning harakatlari sabab yuzaga kelgan deyiladi.

Garchi har bir manzilni aldash ehtimoli oz bo‘lsa-da, lekin katta ommaviy jo‘natish va qamrab olish sababli, fisherlar har bir pochta orqali ma’lum miqdorda qimmatli ma’lumotlarni yig‘ishga muvaffaq bo‘lishadi. Fishing faqat arzon spam-texnologiyalar paydo bo‘lganidan keyin iqtisodiy jihatdan foydali bo‘ldi. Uning paydo bo‘lishidan keyin fishing firibgarlar orasida juda mashhur bo‘lib qoldi. Tadqiqotchilar uning yuqori daromadliligini, murakkabligi, globallashuvi, mijozlarga nisbatan bank, to‘lov va hatto nodavlat tizimlarning keng doiradagi foydalanish imkoniyati va rentAbelligini ta’kidlaydi.

Vishing - fishingga o‘xshash. Faqat bunda jabrlanuvchini soxta veb-saytga jo‘natish o‘rniga, ular bank yoki boshqa ishonchli hokimiyatga tegishli bo‘lgan soxta telefon raqamini izlash talab qilinadi. Telefon orqali suhbatda (yoki qo‘ng‘iroqlarni avtomatlashtirilgan holda) jabrlanuvchidan maxfiy axborot olinadi. IP-telefoniya uchun katta o‘tish sharoitida foydalanuvchi uchun anonim va qiyin ta’qib qilinuvchi telefon raqamini olish oson. Birovning raqamiga, ya’ni asl bank raqamiga qo‘ng‘iroqlarni to‘xtatish mumkin.

Farming - fishingning turi. Farq shundaki, haqiqiy resurs (odatda bankning veb-sayti) ijtimoiy muhandislik usullari emas, balki texnik usullar bilan - DNS-ga hujum qilish, foydalanuvchiga zararli dasturni kiritish va hokazolar yordamida hujumga tutiladi. Shaxsiy ma'lumotlarni uzib qo'yish yanada murakkab yo'l bilan amalga oshirilishi mumkin. Misol uchun, tajovuzkor o'yin-kulgi resursini yaratadi. Ushbu resursda ro'yxatdan o'tayotganda foydalanuvchi elektron pochta manzilini taqdim etishi va parolni tanlashi shart. Ba'zi ehtimollik bilan, foydalanuvchi elektron pochta hisobidagi kabi bir xil parolni ishlatadi. Bu buzg'unchiga jabrlanuvchining elektron manzilini ko'rish imkonini beradi, bu esa maxfiy ma'lumotlarni olishga sharoit yaratadi.

Kiberskvotting. Ushbu atama adolatsiz maqsadda foydalanish yoki boshqa shaxs tomonidan adolatli foydalanishga to'sqinlik qilish maqsadida domen nomini sotib olishni anglatadi. Mamlakatlarning katta qismida domen nomi savdo obyektidir va uning qiymati turli omillarga bog'liq ravishda sezilarli darajada oshishi mumkin. 1980-yilda domen nomlari paydo bo'lgach, ular hech qanday tijorat qiymatiga ega bo'lmaganlar. Lekin 1990-yilning ikkinchi yarmida, "ye-biznes" deb atalmish sanoat rivojlanishi yillarida, bir yaxshi domen nomi mijozlar soni sezilarli darajada ortishiga sabab bo'lishi aniqlangan. Natijada domen nomi qimmatga ega, kompaniya aktivi, sotib olinishi va sotilishi mumkin bo'lgan. Eng mashhur domen nomlarining taxminiy qiymati o'n millionlab dollarlarga yetadi. Domen nomlari bilan bir necha million miqdordagi real operatsiyalar qayd etilgan. Tabiiyki, bunday shartlarda domen nomlarini sotishda daromad qilishga tayyor – kiberskvotterlar paydo bo'ladi.

Internet orqali to'lovlar. Bu, albatta, jinoyat emas. Biroq agar Internet to'lov tizimlari pul o'tkazish uchun ishlatilsa yoki to'lov shartnomasi Internet orqali amalga oshirilsa, ayrim haqiqiy jinoyatlar kompyuterda sodir bo'ladi. Bunday to'lov bilan bog'liq qismda tergov kompyuter sud-texnika texnikasidan foydalanishi kerak. Boshqa tomondan, ko'pgina kompyuter jinoyatlariga bunday tizimlar orqali to'lovlarni amalga oshirish usullari kiradi.

Mamlakat qonunlariga muvofiq va tranzaksiyalarni tekshirish mexanizmlariga ega bo'lgan bank to'lov tizimlari va to'lov usullari bilan bir qatorda, banklar bo'lmagan va davlat organlari tomonidan nazoratga olinadigan shunchaki tarmoq to'lovlari ham mavjud. "WebMoney", "PayPal", "E-gold", "Yandex- Dengi" kabi tizimlarni sanab o'tish mumkin. Odatda, ular turli geytlar (darvozalar) va xususiy vositachilar

bilan o‘zaro bog‘liqdir, shuning uchun tezda bir tizimdan ikkinchisiga mablag‘larni aylantirish mumkin, bu esa jinoiy operatsiyalarni ta’qib qilish va to‘sqinlik qilishni qiyinlashtiradi. Bu tajovuzkorlarni tarmoq to‘lov tizimlaridan foydalanishga undaydi.

Bundan tashqari, ikkinchi darajali xizmatlar - to‘lov tizimlarining hisobini boshqarish, ulardan pul mablag‘larini kiritish va chiqarish, shu qatorda noma’lum bo‘lganlar ham mavjud. Bunday tizimlarning ko‘pligi, ularning transchegara tabiati, pul mablag‘larini bir-biridan uzatishni osonlashtirishi sababli, ham to‘lovchi, ham oluvchiga anonim qolish uchun haqiqiy imkoniyat mavjud. Albatta, bu tom ma’nodagi anonimlik emas, to‘lovlarni kuzatish qiyinligi va kartani rasmiylashtirish uchun rasmiy pasportni taqdim etish yoki uni skanerdan o‘tkazish kerak. Biroq tekshirish rasmiy, kartani boshqa nomga olishda jiddiy to‘siq yo‘q. Bunday tizimdagi akauntlarning erkin sotilishi va xarid qilinishini hisobga olmaganda, pochta orqali yuborilgan kartani buyurtma qilish uchun boshqa birovning hisobidan foydalanish mumkin. Shu kabi imtiyoz, tajovuzkorga jinoiy to‘lovlarni olish uchun "WebMoney" yoki "E-Gold" hisobidan foydalanish, masalan, karderlik faoliyatidan olingan daromad, firibgarlik qurboni yoki tovlamachilik haqini olish imkonini beradi. Elektron pul hamyoniga hisoblangan mablag‘lar, asosan, foydalanuvchini anonimlashtirishga imkon beruvchi hisob boshqaruv interfeysi orqali kartochka hisobiga ikki yoki uch oraliq akkauntdan tezda o‘tkaziladi. Keyinchalik pul bankomatda kartadan yechib olinadi, bu operatsiya ham maxfiylikni ta’minlaydi.

Ushbu usullarni bartaraf etish uchun, vaziyatga qarab, huquqni muhofaza qilish organlari quyidagi vazifalarga duch kelishi mumkin:

- muntazam ravishda buzg‘unchilarning elektron hamyondan naqd pul yechish jarayonini qiyinlashtirish;
- elektron pul jo‘natmalaridan maxsus to‘lovni yechib olishning oldini olish;
- yuboruvchiga ma’lum bir to‘lovni qaytarish;
- muayyan elektron pul hamyonidan pul olgan yoki ma’lum bir to‘lovni olgan shaxsni aniqlash.

Elektron pullardagi pul mablag‘larini qaytarish bo‘yicha yuqorida qayd etilgan kartochkalar to‘lov tizimlari tomonidan emas, (ular o‘z logosini olgan bo‘lsa ham) balki banklar tomonidan beriladi. Banklar mutlaqo hukumatning nazorati ostidadirlar va agar sud sanksiyasi mavjud bo‘lsa, ular kartochka haqidagi barcha ma’lumotni taqdim etish bilan birga, to‘siq qo‘yishi yoki to‘lovni qaytarishi ham mumkin.

Asosiy xulosalar

Kompyuter jinoyat (kiber jinoyat) - tadqiq uchun tabiiy shart axborot texnologiyalari sohasida maxsus bilimlarni qo‘llash hisoblanadigan ma’muriy huquqbuzarlik.

Kompyuter jinoyatlarini ikkita kichik toifaga ajratish mumkin: kompyuter faoliyatiga aralashish bilan bog‘liq jinoyatlar; zaruriy texnik vositalar sifatida kompyuterdan foydalanadigan jinoyatlar.

Kompyuterlar ishiga aralashish bilan bog‘liq jinoyatlarning turlari: ma’lumotlarga ruxsatsiz kirish, dasturiy ta’minotga "mantiqiy bomba"larni kiritish, kompyuter viruslar tarqatish va ishlab chiqish, jinoiy loqaydlik, kompyuter ma’lumotlarini soxtalashtirish yoki o‘g‘irlash.

Jinoyatni sodir etish yo‘li deyilganda jinoyat sodir etilgandan oldin, jinoyat vaqtida va keyin sodir bo‘lgan obyektiv va subyektiv ravishda aniqlangan tizim tushuniladi, bu sudlanuvning mohiyatini, jinoyatchining jinoyat xatti-harakati xususiyatlari, shaxsiy ma’lumotlarini aniqlash uchun sud texnikasi va vositalarini ishlatishga imkon beradigan turli xil izlar qoldiradi. Shunga ko‘ra, jinoyatlarni aniqlash muammolarini hal etishning eng maqbul usullarini aniqlanadi.

Kompyuter jinoyat sodir usullari beshta asosiy guruhga ajratish mumkin: kompyuter texnikasi vositalarini qo‘lga kiritish, axborotni qo‘lga kiritish, undan noqonuniy foydalanish, ma’lumotlar va nazorat qilish buyruqlarini suiste’mol qilish, kompleks usullar.

Aktiv qo‘lga kiritish kompyuterning telekommunikatsion uskunasiga, masalan, printer liniyasiga yoki aloqa kanalining telefon simlariga yoki to‘g‘ridan-to‘g‘ri shaxsiy kompyuterning tegishli portiga ulanish orqali amalga oshiriladi.

Passiv qo‘lga kiritish ko‘plab kompyuter texnikalarining, shu jumladan, aloqa vositalarining ishlashidan kelib chiqadigan elektromagnit nurlanishni aniqlashga asoslanadi.

Kompyuter jinoyat turlari: onlayn firibgarlik, DoS va DDoS hujumlari, zararli dasturlari, defeys, kardertlik, fishing, internet orqali to‘lovlar.

Onlayn firibgarlik sxemasi quyidagilar: axborotni joylashtirish (tarqatish); jabrlanuvchi bilan o‘zaro munosabatlar; pul o‘tkazmasini qabul qilish.

Defeys - bu turdagi jinoyatda tajovuzkor jabrlanuvchining jamoat veb-sayt, ko‘pincha sahifaning nomini o‘zgartiradi.

Kardertlik - bank kartalari sohasidagi firibgarlik.

Fishing- qurbonlarning ijtimoiy muhandislik usullari bilan maxfiy ma’lumotlarini qo‘lga kiritish.

Nazorat uchun savollar

1. *"Kompyuter jinoyati" ni ta’riflang.*
2. *Kompyuter jinoyatlarining asosiy yo‘nalishlari.*
3. *Kompyuter jinoyatlarini tasniflash tuzilmasi.*
4. *Kompyuter jinoyatchilarining odatda tasvirlari.*
5. *Kompyuterlar ishlashiga aralashish bilan bog‘liq asosiy jinoyat turlarini.*
6. *Faol qo‘lga kiritish va passiv qo‘lga kiritish o‘rtasidagi farq nima?*
7. *Kompyuterning maqsadga erishishning "vositasi" bo‘lgan jinoyatlarning qaysi turi mavjud?*
8. *onlayn firibgarlik sxemasini keltiring.*
9. *DoS hujumiga tayyorgarlik ko‘rish va o‘tkazishda texnik jihatdan qanday izlar paydo bo‘ladi?*
10. *Foyda olishga mo‘ljallangan zararli dasturlar.*
11. *Zararli dasturiy ta’minot ishlab chiqarishda qanday raqamli izlarni aniqlash mumkin?*
12. *Bank kartalaridan ma’lumotlarni olish usullari.*
13. *Skiming, real plastik va oq plastik nima?*
14. *Kiberskvotting, fishing nima va uning qanday turlari mavjud?*
15. *Internet orqali to‘lovlarni amalga oshirishda jinoyat turi.*
16. *Kompyuter jinoyatlarining qanday usullari mavjud?*
17. *Axborotni qo‘lga kiritish bilan kompyuter uskunalarini olib qolish o‘rtasidagi farq nima?*
18. *Kompyuter jinoyatlarini sodir etishga olib boradigan asosiy sabablar va shartlar.*

3. KOMPYUTER JINOYATLARINI OLDINI OLISH VA TEZKOR QIDIRUV TADBIRLARI

3.1. Kompyuter jinoyatlarinining oldini olish

Jinoyatchilikka qarshi kurashning xalqaro tajribasi shuni ko‘rsatadiki, zamonaviy jinoyatchilikka qarshi samarali kurashish muammosini hal qilishning ustuvor yo‘nalishlaridan biri huquqni muhofaza qilish idoralari tomonidan turli xil profilaktika choralarini qo‘llashdan iborat. Ko‘plab xorij mutaxassislarining fikricha, jinoyatni oldini olish, uni tavtish qilish va ochishdan osonroq. Odatda kompyuter jinoyatlarining oldini olish bo‘yicha uchta asosiy guruh mavjud bo‘lib, ular butunlay ushbu ijtimoiy xavfli hodisa bilan kurashish uchun ajralmas tizim bo‘lib xizmat qiladi: huquqiy, tashkiliy-texnik va sud.

Ayni paytda, faqat qonunbuzarlik choralari bilan jinoyatchilikning oldini olish bo‘yicha kerakli natijaga erisha olmaydi. Keyingi qadam kompyuter uskunalarini ularga noqonuniy hujumlardan himoya qilish uchun tashkiliy va texnik chora-tadbirlardan foydalanishdir. Afsuski, ko‘plab kompyuter jinoyatlarida korxona va tashkilotlarda yetarli darajada tashkiliy choralar mavjud emasligi, maxfiy ma’lumotlarni ruxsatsiz kirishdan muhofaza qilish zaifligi, maxfiylikning kamligi, zaif tekshiruvlar va xodimlarning yetarlicha yo‘riqnoma olmaganligi ta’sirida sodir bo‘ladi.

Ichki jinoiy ishlar materiallarini tahlil qilish natijasida shu narsa aniq bo‘ldiki, aksariyat hollarda kompyuter jinoyatlarini sodir etishga yordam beradigan asosiy sabablar va shartlar quyidagilardir:

1) xodimlarning moliyaviy operatsiyalar jarayonida dastlabki buxgalteriya hujjatlarini uzatishda uzluksiz ravishda avtonom tarzda va avtomatlashtirilgan tarmoqning ishchi stansiyasi sifatida ishlatiladigan kompyuterning boshqaruv paneliga (klaviaturasiga) nazoratsiz kirish;

2) xizmat ko‘rsatuvchi xodimlarning xatti-harakatlari ustidan nazoratning yo‘qligi, bu jinoyatchiga jinoyat sodir etish vositasi sifatida kompyuterdan erkin foydalanish imkonini beradi;

3) kiritilgan axborotning muvofiqligi va to‘g‘riligini tekshirishni ta’minlaydigan, sinov xavfsizligi bo‘lmagan dasturiy ta’minotning past darajasi;

4) foydalanuvchining shaxsiy biometrik parametrlari bo‘yicha ishonchli identifikatsiya qilinishini ta’minlaydigan, ishchi stansiyasiga

va uning dasturiy ta’minotiga ruxsatsiz kirishdan himoyalovchi parolni himoya qilish tizimining nomaqbulligi;

5) kompyuter texnikasini ruxsatsiz foydalanishdan himoya qilish nuqtai nazaridan tijorat axborotining maxfiyligi hamda uning xavfsizligini ta’minlash uchun mas’ul mansabdorlarning belgilanmaganligi;

6) xodimlardan qat’iy moliyaviy hisobotlarni, shu jumladan, mashina ma’lumotlari shaklidagi hujjatlarni rasmiy ravishda qabul qilinmasligi;

7) xodimlar bilan savdo va xizmat sirlarini, shaxsiy ma’lumotlarini va boshqa maxfiy ma’lumotlarni oshkor qilmaslik to‘g‘risidagi shartnomalarning (kontraktlar) yo‘qligi.

Kompyuter jinoyatchilikka qarshi eng samarali himoya qilish, tashkilotning shtat jadvaliga kompyuter xavfsizligi bo‘yicha mutaxassis lavozimini joriy etish (ma’lumot himoyasi bo‘yicha administrator) yoki vaziyatdan kelib chiqqan holda xususiy yoki markazlashgan maxsus xizmatlardan foydalanish hisoblanadi. Chet ellik mutaxassislarning fikriga ko‘ra, bunday bo‘linma (xizmat) ning mavjudligi kompyuter jinoyatlarining sodir qilish ehtimolini ikki marta kamaytiradi.

Tashkiliy-boshqaruv choralari ichida texnik chora-tadbirlar (apparat, dasturiy ta’minot va kompleks) muhim ahamiyatga ega. Texnik usul kompyuter jihozlarini kiruvchi jismoniy ta’sirlardan himoya qilish va maxfiy axborotning qochqin kanallarini yopish uchun mo‘ljallangan. Ular orasida uzluksiz quvvat manbalari, apparatni himoya qilish vositalari, qulflar va shaxsiy identifikatsiyalash moslamalari mavjud. Dasturlarni muhofaza qilish usullari axborotni to‘g‘ridan-to‘g‘ri himoya qilish uchun mo‘ljallangan. Ma’lumotni uzatishda ma’lumotni himoya qilish uchun odatda ma’lumotlar shifrlashning turli usullari qo‘llaniladi. Amaliyotga ko‘ra, shifrlashning zamonaviy usullari xabarning ma’nosini ishonchli tarzda yashirishi mumkin. Axborot resurslarini dasturiy ta’minoti bilan bog‘liq masalalarni ko‘rib chiqishda, kompyuter jinoyatlarini sodir etish usuli sifatida ularni himoya qilish muammosi ta’kidlangan. Hozirgi vaqtda antivirus dasturiy ta’minoti ishlab chiqarilmoqda, bu zararli dasturiy ta’minotni va uning tarkibiy qismlarini aniqlash uchun ba’zi bir muvaffaqiyatlarga (taxminan 97%) ega bo‘lish imkonini beradi. Mavjud antivirus dasturiy paketlari (Kaspersky, AIDSTEST, DrWeb, SHERIFF, ADinf, Norton Antivirus va boshqalar) virusli dasturlarning aksariyatini aniqlash va yo‘q qilish uchun qo‘l keladi.

3.2. IP-manzilining tegishliligini va joylashuvini aniqlash

Internet bilan bog‘liq deyarli har bir jinoyat ishi bunday muammoni o‘z ichiga oladi: ma’lum IP- manzil bo‘yicha foydalanuvchi kompyuterni va uning joylashuvini aniqlash.

Odatda, bunday dalillar quyidagilarga o‘xshaydi:

(jinoyat) — (IP-manzil) — (kompyuter) — (inson)

Turli texnik vositalar yordamida jinoyat sodir etilgan IP-manzil qayd etiladi. S3.4.o‘ng, kompyuter qo‘llagan IP manzil aniqlanadi va bu fakt ekspertiza yordamida isbotlanadi. Shundan so‘ng, gumonlanuvchi ushbu kompyuterni tegishli vaqtda nazorat qilganini isbotlashi kerak.

IP-manzil Internetdagi kompyuter yoki boshqa qurilma uchun noyob identifikator hisoblanadi. Bu shuni anglatadiki, bir vaqtning o‘zida butun global kompyuter tarmog‘ida faqat bitta kompyuter ma’lum bir IP-manzilni ishlatishi mumkin. Ushbu qoidaga bir qator istisnolar mavjud:

- maxfiy yoki "kulrang" deb ataluvchi IP-manzillar;
- ommaviy yoki ko‘p kastli (multicast) IP-manzillar;
- tarmoq va keng eshittirish (broadcast) IP manzillari;
- alohida belgilanmagan yoki registratdan berilmagan IP-manzili;
- kompyuterlarning geografik taqsimlangan klasterlari bilan bog‘liq IP manzillar.

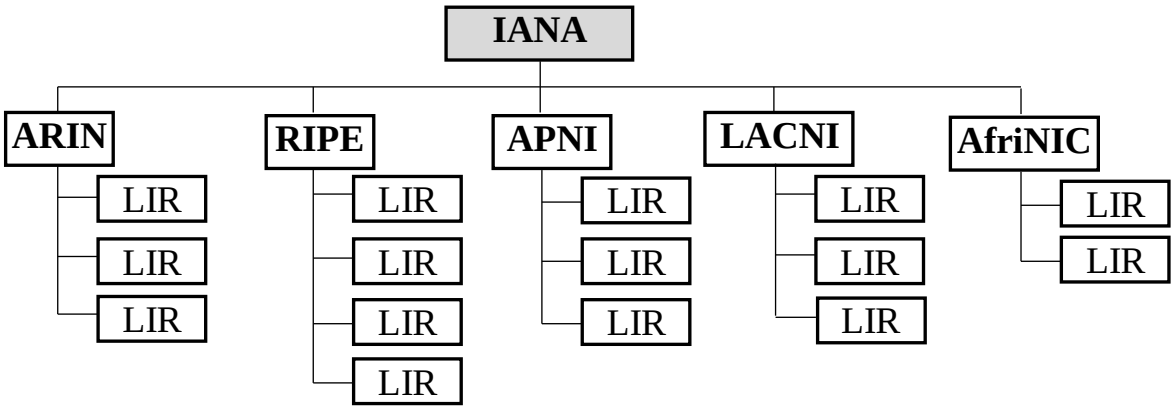
IP-manzil umumiy manzili toifasiga tegishli bo‘lsa ("oq" deb ataluchi), u registratdan berilmagan bo‘lsa, bu manzil marshrutlashadi. Buning mazmuni shuki, ushbu manzilga Internetning istalgan nuqtasidan yuborilgan IP-paket o‘z manzilini topadi. Boshqacha qilib aytganda, IP manzil noyobdir va bu IP-manziliga ega bo‘lgan kompyuterni sozlash mumkin.

IP-manzili noyobligi yoki noyob emasligi, yuqorida aytilgan istisnolarga kirish yoki kirmasligi - bu mutaxassis tomonidan belgilanadi.

Registratorlar. Internetda IP-manzillarni taqsimlash va IP-manzillari ro‘yxatdan o‘tkazish bilan shug‘ullanuvchi tashkilotlar IP registratorlar (IP Registry) deb ataladi. Bu tashkilotlar Internetning o‘z-o‘zini boshqarish organlari hisoblanadi. Registratorlar uch darajali iyerarxiyani hosil qiladi: IANA — RIR — LIR.

IANA ni tashkillashtirish asosiy registrator hisoblanib, hududiy registrator va katta tashkilotlarga IP-manzillarning eng ulkan IP-manzillar blokini ajratadi.

Hozirda mintaqaviy registratorlarning (RIP) soni 5 ta (12-rasm).



16- rasm. Mintaqaviy registratorlar

Bular ARIN (Shimoliy Amerika), RIPE (Yevropa va Markaziy Osiyo), APNIC (Osiyo-Tinch okeani hududi), LACNIC (Lotin Amerikasi), AfroNIC (Afrika). Ular mahalliy registratorlarga o‘rta va yirik address bloklarini berishadi, shuningdek belgilangan IP-manzil ma’lumotlar bazasini yuritadi va unga kirish huquqini beradi.

Mahalliy registratorlar (LIP) kichik IP-manzil bloklarini aloqa operatorlari va foydalanuvchilarga beradi hamda o‘zining mahalliy registrator ma’lumotlar bazasida ro‘yxatga oladi. Odatda, mahalliy registrator vazifasi aloqa operatori (internet provayder) bajaradi. Bundan registratorlarning soni bir necha minglabdir.

Barcha IP-manzillar mahalliy registrator (RIR) qo‘llab-quvvatlovchi maxsus ma’lumotlar bazasida ro‘yxatdan o‘tadi. Ushbu bazadagi ma’lumotlar (bir necha maydonlar bundan istisno) whois protokoli bo‘yicha istalgan shaxs uchun ochiqdir. Bu bazaga murojaat etish oson. Internetga ulangan holda, buyruqlar satriga «whois <ip-manzil>» ni kiritish lozim. Ushbu buyruq Windowsdan tashqari barcha operatsion tizimlarda mavjud. Undan foydalanish noqulay bo‘lgan yoki imkoniyati mavjud bo‘lmaganlar uchun brauzer yordamida so‘ralgan IP-manzilni kiritish va kerakli ma’lumotlar bazasidan foydalanish mumkin bo‘lgan veb-interfeyslar, ya’ni veb sahifalar mavjud.

Olingan ma’lumotlarga shu tarzda ishonish mumkinmi? Yozishni yaratish, o‘zgartirish va yo‘q qilish bo‘yicha javobgarlik mahalliy registratorlar (LIR) bo‘ynidadir. Biroq bu vazifalarni bajarish qat’iy ravishda monitoring qilinmaydi. Mahalliy registr yozuvni vaqtincha

yangilab turishi yoki uning ishini yengillashtirish uchun bir nechta mijozlarga ajratilgan bir qator manzillarni yozib qo‘yishi mumkin. Bundan tashqari, IP- manzil foydalanuvchilari, odatda mijozga ko‘ra, to‘g‘ri tekshiruvlarsiz kiritiladi. Bularning barchasi ma’lum ma’lumotlar bazasi yozuvlari orasida noto‘g‘ri - eskirgan ma’lumotlar tarqalishiga olib keladi.

Shuning uchun bunday ma’lumotlarga to‘liq ishonish kerak emas. Odatda, mahalliy registratorlar (LIR) to‘gri ma’lumotga ega bo‘ladi, negaki u mintaqaviy registrator (RIR) bilan shartnoma tuzgan, a’zolik badallari to‘laydi, doimo o‘zaro hamkorlik qiladi. Va RIR mijozi darhol IP-foydalanuvchisi haqida ma’lumot tekshirilishi lozim.

Qo‘lga tushmas IP. Yana bir qiziq misol keltiramz. Bu "zombi hosting", ya’ni, jamoatchilik tarmoq resurslarining serverlarda emas, balki zombi tarmog‘i (botnet) kompyuterlarida saqlanishidir. Zombi mijoz kompyuterlari ham veb-serverlar sifatida, ham tegishli domen uchun DNS-serverlar sifatida ishlatiladi. Zombi-server uzoq vaqt yashamaydi - bir necha soatdan bir necha kungacha. Biroq ularning soni juda ko‘p. Shuning uchun doimiy kirishni saqlab qolish mumkin.

Bunday saytning joylashuvini tuzatish mumkin emas, egasini topish juda qiyin va bunday sharpa-saytini boshqarish haqiqatini isbotlash ham oson emas.

Ta’riflangan texnologiya juda kam qo‘llaniladi. Veb-saytlarning aksariyati barqaror IP-manzillarda yashaydi, operator-egalari saytning egasi haqida bilmasa, uning kamida joylashganligidan xabardor bo‘ladi.

Fazo va vaqt. IP-manzillari bitta foydalanuvchidan boshqasiga o‘tishlari mumkin. Ulardan ba’zilari doimiy ravishda namoyon bo‘ladi - ular statik deb nomlanadi. Boshqa IP-manzillar faqat ma’lum bir aloqa sessiyasi uchun ajratilgan va dinamik deb ataladi. Statik IP-manzillar uchun umr davri bir necha oy va yillar, dinamik IP uchun esa daqiqa uchun hisoblanadi.

Bu, odatda, dinamik ajratish uchun ishlatiladigan IP-manzil intervallari uchun yozuvlarda ko‘rsatiladi. U yerda "dynamic", "dialup" yoki "NAT" so‘zlarini ko‘rish mumkin.

Har ikkala holatda ham, IP-manzillarning egalik huquqini belgilashda ushbu manzilni foydalanuvchini o‘rnatmoqchi bo‘lgan vaqtni hisobga olish kerak. Dinamik IP-manzillar uchun ushbu vaqt qisqa sekunddagi aniqlik bilan aniqlanishi kerak, chunki qisqa muloqot sessiyalari mavjud. Vaqtdan tashqari, vaqt zonasi va mumkin bo‘lgan xatolar qayd etilishi kerak.

Hujjatlashtirish. Jinoiy ish uchun, odatda, faqatgina whois serverining javobini chop etish yetarli bo‘lmaydi. RIPE Yevropa mintaqaviy Registratoridan rasmiy hujjatni olish juda qiyin bo‘ladi.

Mavjud amaliyot whois server javobini hujjatlashning ikki yo‘lini beradi. Birinchi variant: bunday javobni chop etish mahalliy lokal registrator (LIR) bo‘lgan mahalliy telekommunikatsiya operatori tomonidan tasdiqlanishi mumkin. Ikkinchi variant: IP-manzilga egalik huquqi haqida ma’lumot ma’sul xodim bildirgisi bilan olish; Registr ma’lumotlar bazasidan ma’lumotlar to‘g‘ridan-to‘g‘ri hisobot matnida taqdim etiladi. Hujjatlarning boshqa variantlari (tekshiruv, notarial tasdiqlash, RIR dan olingan ma’lumot) amalda mavjud, lekin shu paytgacha qo‘llanilmagan emas.

IP-manzilning muayyan kompyuterga tegishliligi ushbu kompyuterning ekspertizasi va telekommunikatsiya operatori xodimlarining ko‘rsatmalari bilan tasdiqlanishi kerak. Shuning uchun, whois-server javobini hujjatlashtirishda ta’riflangan qat’iylik yetishmasligi maqbuldir.

Jismoniy joylashuv. Ro‘yxatga oluvchining ma’lumotidan IP-manzil diapazoni yoki ichki tarmoqlar kimga tayinlanganligini bilib olamiz. Odatda bunday subyekt telekom-operator yoki uning mijozidir. Ro‘yxatga oluvchining ma’lumotlar bazasida kamdan-kam hollarda IP-manzilning darhol foydalanuvchisi paydo bo‘ladi.

Favqulotda foydalanuvchi haqida ma’lumotlarni olish yoki aniqlashtirish, shuningdek, tegishli IP-manzil ro‘yxatdan o‘tgan telekommunikatsiya operatoridan geografik joylashuvini aniqlash mumkin. Ushbu operator mijozning aniq manzilini bilmasligi mumkin, chunki u va mijoz o‘rtasida vositachisi yoki vositachi-operator mavjud bo‘ladi. Ba’zan bunday vositachi soni birdan ko‘proqdir. Bu holatda, operatorlarning barcha zanjiri orqali o‘tishga to‘g‘ri keladi.

Ma’lumki, IP-manzillar egaligini belgilash vazifasini, barcha mumkin bo‘lgan xususiyat va qiyinchiliklarni qayd etish va eslatish mumkin emas.

Shuning uchun TQT yoki dastlabki tergov jarayonida IP-manzilning joylashishini aniqlashda texnik mutaxassis ishtirok etishi shart.

3.3. Domen nomining tegishliligini aniqlash

Domen - noyob nom bilan belgilanadigan Internet iyerarxik maydonidagi hudud (shox). Ba’zi yuristlar domen nomini

shaxsiylashtirish vositalari bilan bog‘lashadi. Boshqalar uni bunday deb o‘ylamaydi va domen nomining huquqiy tabiati hali aniq aniqlanmagan deb aytishadi. Hatto noodatiy qarash ham mavjud – bu elektroaloqani raqamlash resursidir.

Qonuniylikdan farqli o‘laroq, domen nomlarining texnik tabiati yaxshi ma’lum va aniq texnik standartlarda belgilangan.

Domen nomi maydonini adolatli taqsimlash va ularning global yagonaligini ta’minlash uchun domen nomlarini ro‘yxatga olish tizimi mavjud. Barcha birinchi darajali domen nomlari (masalan, org, info, ru, ua), barcha ikkinchi darajali domen nomlari (masalan, gprf.info, fnn.ru) va ayrim uchinchi darajali taniqli domen nomlari (masalan, provider.net.ru, london.co.uk) ro‘yxatdan o‘tishi lozim. Boshqa domen nomlari ro‘yxatdan o‘tkazilishi shart emas va yuqori domen egasining ixtiyoriga ko‘ra taqsimlanadi (misol uchun, www.fnn.ru va mail.fnn.ru domenlari fnn.ru ikkinchi darajali domen egasi ruxsati bilan yaratiladi va foydalaniladi).

Majburiy ro‘yxatga olingan har bir domen uchun registrator yoki bir nechta registratorlar tayinlanadi. So‘nggi holatda barcha registratorlar ro‘yxatga olingan domen nomlarining yagonaligini ta’minlash uchun yagona ma’lumotlar bazasidan foydalanishga majburdirlar. Barcha registratorlarning ma’lumotlar bazalari IP manzillari registratorlariga o‘xshagan whois protokoli orqali ommaga ochiqdir. Ro‘yxatdan o‘tgan domen foydalanuvchilardan birini topish uchun, u qarashli bo‘lgan registrator ma’lumotlar bazasiga murojaat etish kerak. Ro‘yxatga olinmagan domen nomlari uchun yuqoriroq darajadagi tegishli domen egasiga murojaat qilish lozim.

Masalan, biz "www.internet-law.ru" 3-darajali domen egasini aniqlashimiz zarur. Shubhasiz, bu 3-darajali domen ro‘yxatdan o‘tgan domen emas. Bu mulk egasining tasarrufida bo‘ladi 2-darajali domen, ya’ni allaqachon ro‘yxatdan o‘tgan “internet-law.ru” domenidir. Bu yerda taxmin qilish kerak, ya’ni standart nomga (www) ega 3-darajali domenning egasi 2-darajali domenga ham egalik qiladi, "internet-law.ru" domen nomini bilib olish uchun biz rus registratorlari bazasiga murojaat qilamiz. Buning uchun har qanday operatsion tizimda (Windows tashqari) mavjud bo‘lgan "whois" buyrug‘idan foydalaniladi. Argument sifatida xohlagan domen nomi belgilanadi va parametr qaysi registr so‘ralayotganini belgilab qo‘yadi. Registratorning ma’lumotlar bazasiga domen egasi ma’lumotlarini kiritishi esda tutilishi kerak. RU domenida va boshqa domenlarda registrlarni ro‘yxatga olish va o‘zgartirish tartibi

o‘rnatiladi. Albatta, ma’lumotlarning dolzarbligi va ishonchliligi uchun talablar mavjud. Biroq registratorlar har doim o‘zlariga taqdim qilingan ma’lumotlarni tekshirish imkoniga ega emaslar. Va eskirgan narsalarni yangilash doimo o‘z vaqtida amalga oshirilmaydi.

Domen egasi to‘g‘risida qanday ma’lumotlar ishonchli deb hisoblanishi mumkin? Domen nomini nazorat qilish huquqi bilan bog‘liq ko‘pchilik registratorlarning odatiy shartnomasi shartlariga ko‘ra, domen nomining egasi to‘g‘risida noto‘g‘ri ma’lumotlar ko‘rsatilgan holda, ro‘yxatdan o‘tkazish bekor qilinadi. Ko‘rsatilgan aloqa ma’lumotlariga murojaat qilmaslik domen nomlari huquqlarining yo‘qolishiga olib kelishi mumkin. Ko‘pgina registratorlar avvalgi egasiga tegishli hujjatlarni taqdim etguniga qadar domen nomlarini boshqa shaxsga o‘tkazishga ruxsat bermaydi. Shuning uchun noto‘g‘ri aloqa ma’lumotlari (telefon, pochta manzili, e-mail manzili) katta ehtimollik bilan ko‘rsatilganligi domen nomining yo‘qolishiga olib keladi. Egasining noto‘g‘ri ismini belgilash domenni boshqa egasiga (sotishga) o‘tkazish mumkin emasligiga olib keladi.

Yuqoridagilardan kelib chiqib foydalanuvchi to‘g‘risidagi qaysi ma’lumot haqqoniy, qaysinisi esa ishonchsizligi to‘g‘risida xulosa qilish mumkin. Domenga egalik huquqini hujjatlashtirish bilan shug‘ullanish biroz murakkabliklar keltirib chiqaradi. Jinoyatchi va fuqarolik jarayoni uchun bunday domen nomining ma’lum shaxsga tegishli ekanligini ko‘rsatish muhim sanaladi. Amaliyotda quyidagi usullar qo‘llaniladi:

1. Ma’sul shaxsdan bildirgi orqali whois serveridan yordam olish uchun hujjat tayyorlash. Bu mukammal usul emas. Faqat ayblanuvchi (sudlanuvchi) domen egalik huquqini inkor etish niyatida bo‘lmasa qo‘llanilishga maqbul.
2. Notariusda whois komandasining veb-interfeysi bo‘lgan veb-sahifaning mazmunini tasdiqlatish. Fuqarolik ishlari uchun foydalaniladi. Notarial idoralar veb-sahifalar mazmunini tasdiqlashni qabul qilmaydi. Biroq agar bunday notarius topilsa, notarius guvohiligi sudda ijobiy taassurot qoldiradi. Lekin mutaxassis uchun bu usul noto‘g‘ridir, chunki notarius qanday ma’lumotlar bazasi veb-interfeysga bog‘langanligini ko‘rmaydi. Natijada, uning ishonchi, allaqanday maqsadda noma’lum kimsaning chetiga yozilgan yozuvning kafolatidan ortiq emas.
3. Ushbu domen nomini saqlab qolish bilan bog‘liq xizmat ko‘rsatuvchi aloqa operatori (provayder) rasmiy javobini olish, masalan, u uchun DNS-server yoki veb-saytni qo‘llab-

quvvatlaganligi. Provayderdan xat o‘rniga ushbu provayderning tegishli texnik xodimidan guvohlik olish mumkin.

4. Guvohlardan ko‘rsatuv olish. Misol uchun, manfaatdor shaxs domen nomi bilan faqat uning egasiga tegishli bo‘lgan muayyan xatti-harakatlarni amalga oshirganligi to‘g‘risida.
5. Tegishli shaxs ro‘yxatga olish yoki domenni yangilash xizmatlarini to‘laganligini tasdiqlash. Birovning domenlariga pul o‘tkazish mumkin bo‘lsada, ammo baribir bu juda yaxshi bilvosita dalil.
6. Mutaxassis whois serveriga so‘rov yuborib, natijalar haqida o‘z xulosasida bayon qiluvchi ekspertiza o‘tkazish. Uslub oddiy, ammo mukammal emas. O‘rganiluvchi obyekt (registrator ma’lumotlar bazasi, whois serveri) dunyoning narigi burchagida, hech kim aniq bilmaydigan yerda va mutaxassisdan yiroqda bo‘lishi hisobga olinsa, ekspertiza o‘tkazish fikri ikkilanarlidir.
7. Tegishli shaxsning kompyuterida eskpertiza davomida domen registratori interfeysiga muvaffaqiyatli avtorizatsiyalash izlarini topish. Bu domen registrator interfeysida ulanish va muvaffaqiyatli avtorizatsiyadan dalolat beradi. Deyarli barcha registratorlar domen nomlari egalarini o‘z veb-interfeysi orqali o‘zlarining domenlarini masofadan boshqarish qobiliyatiga ega bo‘lishadi.
8. Domen nomini ro‘yxatdan o‘tkazish to‘g‘risidagi sertifikatni tegishli ro‘yxatdan o‘tkazuvchi yoki texnik markazdan olish. Chet ellik registratorga bunday sertifikatni olish qiyin. Bunda Interpol xizmatlaridan foydalanishga to‘g‘ri keladi.

3.4. Elektron pochta manzilining tegishliligini aniqlash

Elektron pochta xabarlari bir qancha jinoiy va fuqarolik ishlarida aks ettirilgan. Ba’zilarda hatto markaziy dalillar deb hisoblanadi. Elektron pochta orqali amalga oshiriladigan bitimlar yordamida jinoyat sodir etishda fitna uyushtirish, tovlamachilik sodir etilib, ish uchun ahamiyatli ma’lumotlar keltiriladi. Bu kabi holatlarda savol tug‘iladi: e-pochta manzil kimga tegishli yoki undan kim foydalanadi?

Pochta qutisi. Ko‘pgina hollarda elektron pochta manzili pochta qutisi bilan bevosita bog‘liq. Ushbu manzilga yuborilgan barcha xatlar ushbu qutiga tushadi va undan foydalanuvchi uni olib qo‘yishi mumkin.

Biroq istisnolar mavjud:

– pochta yoki pochta manzili roʻyxati boʻlgan guruh yoki guruh manzillari; ushbu manzilga yuborilgan barcha xatlar ma’lum bir manzil adresatidan yuboriladi; Odatda bunday manzillar, masalan, info@company.ru yoki noc@provider.net deyiladi;

– texnik manzillar orqasida, na foydalanuvchi, na pochta qutisi turadi; Bunday manzilga kelgan barcha xatlar dastur tomonidan qayta ishlanadi; masalan, ba’zan qaytish manzili noreply@domain.com kabi koʻrsatiladi - bu manzilga kelgan hamma narsa pochta serveri tomonidan /dev/null qurilmasiga yuboriladi;

– qayta joʻnatish (forward) xabarlar uchun manzillar; Bunday manzilga kelgan barcha xabarlar pochta qutisiga qoʻshilmaydi, ammo oldindan belgilab qoʻyilgan manzilga qayta yoʻnaltiriladi.

Xabarlarni **yuborish.** Elektron pochtada manzil quyidagi sohalarda koʻrsatilishi mumkin.

Qabul qiluvchining manzili - "To", "Cc" va "Bcc" maydonlarida.

Yuborgan - maydon «From» ham, «Reply-to» va «Return-path». Gʻayritabiiy jihati shundaki, yuqoridagi barcha maydonlarda haqiqiy manzil boʻlmasligi mumkin. Barcha oltita manzillar soxta boʻlishi mumkin, ammo shunga qaramasdan xabar egasiga yetadi.

Oʻrnatish. Avval manzilni bogʻlaydigan pochta qutisini belgilash kerak. Keyin kim ushbu pochta qutisidan foydalanishini topish lozim. Bu manzil egasini belgilaydi. Pochta qutisi joylashuvini oʻrnatish uchun tadqiqotchi asosiy domenni oʻrnatadi. Koʻpgina hollarda quti bir xil serverda joylashgan. Boshqa hollarda, server oʻz parametrlarida koʻrsatilgan boshqa serverga xat joʻnatadi. Har ikkala holatda, pochta qutisining oʻrnini aniqlash uchun ushbu sozlamalarni bilish talab etiladi.

Bu serverga xizmat koʻrsatuvchi provayder yordamini talab qiladi. Pochta qutisi joylashuvi kerakli server (serverlar) ning tekshiruv protokoli yoki ekspert xulosasi bilan hujjatlashtiriladi. Oxirgi chora sifatida provayder tomonidan tegishli soʻrovga yozma javob olishni cheklab qoʻyish mumkin, ammo bu isbotlash usuli mukammal deb nomlana olmaydi. Quyidagilar pochta qutisi ma’lum bir shaxs tomonidan ishlatilganligini tasdiqlovchi dalillar boʻlishi mumkin:

– ushbu qutiga kirish uchun sozlamalarning ushbu shaxsning kompyuterida mavjudligi (parolni oʻz ichiga oladi);

– foydalanuvchi kompyuterida ushbu pochta manzilidan oʻtganlikni bildiruvchi, xizmat sarlavhalariga ega xatlarning mavjudligi;

– pochta mavjud bo‘lgan serverda ushbu pochta qutisining muvaffaqiyatli ulanish va foydalanuvchi autentifikatsiyasi haqida ma’lumot beruvchi loglarning mavjudligi;

– boshqa abonentlarida ushbu pochta qutisiga yuborilgan xabarlarga javob sifatida yozilgan xabarlar (asl xabar ko‘pincha javobda ko‘rsatiladi, shuningdek, xizmat sarlavhalarida oldingi xabarlarga havolalar mavjud bo‘ladi) mavjudligi.

3.5. Whois nima?

Hozirda Internet shu darajada yashirinki, siz suhbatdoshingiz devor orqasidagi do‘stingiz bo‘lishi mumkinligini yoki sizning xotiningiz sizning sevimli forumingizdagi eng shiddatli raqibingiz bo‘lishini bilmasligingiz mumkin. Lekin har doim ham anonimlik maxfiy bo‘lmaydi. Internet-resurslarning egalarini ifodalovchi " **Whois"** xizmati mavjud. "**Whois**" ***termini*** *nima?* Aslida, hamma narsa oddiy. Bu serverga domenni ro‘yxatdan o‘tkazgan yoki unga tegishli bo‘lgan **IP-manzil** ma’lumotni mijozga uzatishi mumkin bo‘lgan protokoldir. Ma’lumotlar ma’lum domen foydalanuvchilari haqidagi ma’lumotlarni o‘z ichiga olgan maxsus ma’lumotlar bazalari bilan taqdim etiladi. Tabiiyki, bu ma’lumotlar eskirgan yoki ishonchsiz bo‘lishi mumkin, chunki bu ma’lumotlar domenni ro‘yxatdan o‘tkazishda shaxs tomonidan taqdim etiladi. Ushbu ma’lumot shuningdek batafsil bo‘lishi mumkin: ma’lumotlar bazasida foydalanuvchi nomi, ro‘yxatdan o‘tish manzili, elektron pochta, telefon raqami va ushbu domenni ro‘yxatdan o‘tgan kompaniya nomlari mavjud. Bularning barchasi IP manzil ma’lumotlariga ham mos keladi.

Nima uchun Whois protokoliga muhtojlik bor? Internet rivojlanishi boshlagan va kiberskvotting kabi muammo haqida hech kim eshitmagan paytlarda, sayt ma’murlari uni bir-biriga kerakli ma’lumotlarni topish va turli muammolarni hal qilish uchun foydalanishi mumkin deb taxmin qilinardi. Ayni paytda, ko‘pincha kiberskvottinlarni ushlash va ularga qarshi kurashish talab etiladi. Whois protokoli bilan ishlash uchun turli dasturlar (mijozlar) mavjud. Ulardan ba’zilari konsol interfeysi, boshqalari esa grafikdir, lekin ko‘pincha veb-interfeys orqali ishlaydi, ya’ni, domenlar va IP-adreslar haqida ma’lumot olish brauzerlardan foydalanish kabi amalga oshiriladi. Yandex, Google yoki boshqa qidiruv tizimi yordamida topish va foydalanish oson bo‘lgan ko‘plab **Whois xizmatlari** mavjud. Aksariyat xizmatlar ma’lumotlar bazalari

xususiyatlarining mavjudligi sababli, Whois ma’lumotlarini izlash uchun mo‘ljallangan ba’zi domen hududlari bilan cheklanadi.

Domen foydalanuvchilari va IP-manzillar to‘g‘risidagi ma’lumotni o‘z ichiga olgan ma’lumotlar bazalari tarqatilishi yoki markaziy ravishda dunyodagi barcha domenlar yoki IP-manzillar haqidagi ma’lumotlar mavjud bo‘lmagan yagona ma’lumotlar bazasi mavjud emas. Markaziy ma’lumotlar bazalarida (ORG domen zonasida) hamma narsa juda oddiy: bitta server barcha Whois so‘rovlariga javob beradi va u barcha zarur ma’lumotlarga ega.

Ma’lumotlar bazasi markazlashtirilmagan bo‘lsa (COM domen zonasi), server so‘rovlarni cheklangan miqdordagi domenlar haqida ma’lumotga ega bo‘lgan boshqa serverlarga yuboradi. Bugungi kunda markazlashtirilgan ma’lumotlar bazalari ko‘pgina domenlar mavjud bo‘lgan domen zonalarida qo‘llaniladi, tarqatilganlar katta domen zonalari uchun mos keladi (umuman ORG va COM misolida ham ko‘rish mumkin).

Agar siz hamkasbingiz yoki veb-ishlab chiquvchi orqali ro‘yxatdan o‘tgan bo‘lsangiz, Whois xizmatiga murojaat qilib bu unga tegishli ekanligini tekshiring.

Agar domen do‘stlar orqali ro‘yxatga olingan bo‘lsa va muhim ma’lumotlar - parol, foydalanuvchi nomi yo‘qolsa, sizning domeningizni abadiy yo‘qotishi mumkin. Uning imkoniyatlari sizning raqobatchilaringizni nazorat qilishda va foydalanadigan strategiyasini va Internetni tushunishda yordam beradi va ularni bartaraf etish uchun javob choralarini ishlab chiqadi.

3.6. Log-fayllarni o‘rganish

“Log fayllari” yoki oddiygina **"loglar"** iboralari jarayonning barcha ishtirokchilari tomonidan operativ guruh a’zolari, tergovchilar tomonidan osonlikcha ishlatiladi, biroq ulardan ozchiligi nima ekanligini aniq tasavvurga ega. Logda qanday ma’lumot saqlanadi? Har qanday! Qaysinisini, istagingizni, xohlaganingizni yozib oling.

Shunday qilib, log-fayl yoki log nima?

Log - dasturda saqlanadigan avtomatik voqea jurnali. Odatda har bir voqea jurnaldagi bitta yozuvga mos keladi.Odatda, qaydlar voqea hodisadan (uning boshlanishi yoki oxiri) keyin darhol amalga oshiriladi. Ushbu qaydlar dasturning o‘zi tomonidan belgilangan faylga qo‘shiladi yoki u tomonidan jurnallarni saqlash uchun mo‘ljallangan boshqa maxsus dasturga yuboriladi.

Ushbu ta’rifidan shu narsa aniq bo‘ldiki, har qanday hodisalar – masalan, bitta Ethernet-freymdan prezident saylovlarida ovoz berish natijalariga qadar jurnallarda qayd etilishi mumkin. Tadbirning shakli ham dastur muallifining ixtiyoriga ko‘ra tanlanadi. Jurnal formati mashinaga yo‘naltirilgan bo‘lishi yoki u odamlar o‘qishi uchun moslashtirilishi mumkin.

Ba’zan loglar xavfsizlik maqsadlariga va hodisalar bo‘yicha tekshiruvlarga yo‘naltirilgan. Bunday hollarda, iloji bo‘lsa, tizimdan qaydlarni, ular saqlagan voqealarni izolyatsiya qilishga harakat qilinadi. Agar tajovuzkor tizimning himoya tizimidan o‘tsa va tizimga kirishni boshlasa, u izlarini yashirish uchun bir vaqtning o‘zida loglarga kirishga qodir emas.

Axborot tizimiga ta’sir o‘tkazishda deyarli har bir inson harakatlari logga bevosita yoki bilvosita, ba’zida hatto bir nechta loglarda ham aks ettirilishi mumkin. Va bu loglar turli joylarda tarqalib ketishi mumkin, bu haqda mutaxassis bo‘lmagan shaxs taxmin qila olmaydi.

Tajovuzkorning xatti-harakatlari haqida ma’lumot olish uchun, unga tegishli ma’lumotlardan foydalanish uchun quyidagilarni amalga oshirish kerak:

– kompyuterlar va ularning dasturlari o‘zaro hamkorlikda ishtirok
– etishlarini aniqlash;
– tegishli dasturlarning har birida qaysi hodisalar qayd
– etilganligini aniqlash;
– tegishli belgilangan vaqt uchun belgilangan barcha loglarni olish;
– bu loglardagi yozuvlarini o‘rganib, ularni bir-biri bilan
– solishtirish.

Bir foydalanuvchining bitta veb-sahifani ko‘rib chiqishi kabi oddiy faoliyatni misol qilib keltirish mumkin. Keling, ushbu tadbirda ishtirok etadigan tizimlarni ro‘yxatga olaylik, ular asosan voqea loglarida saqlanishi mumkin:

– foydalanuvchi brauzeri;
– foydalanuvchining kompyuterida shaxsiy xavfsizlik devori;
– foydalanuvchining kompyuterida antivirus dasturi;
– foydalanuvchi operatsion tizimi;
– veb-sahifani so‘rashdan avval, foydalanuvchining brauzeriga kirgan DNS-serveri (*resolver*) hamda bu resolver murojaat qilgan server;

– barcha routerlar foydalanuvchi kompyuteridan veb-serverga va DNS-serverlar, shuningdek, ushbu routerlarning statistikasini jo‘natadigan billing tizimlar;

– veb-server va tegishli DNS-serverlarga qarshi himoya (xavfsizlik devori, hujumni aniqlash tizimi, antivirus);

– veb-server;

– veb-server tomonidan boshqariluvchi CGI-skriptlari;

– foydalanuvchi tomonidan ko‘riladigan veb-sahifada joylashgan barcha hisoblagichlarning veb-serverlari va banner reklamalari (odatda, ular mustaqil provayderlar tomonidan qo‘llab-quvvatlanadi);

– foydalanuvchining ko‘rilgan sahifadan giperhavola orqali ketayotgan veb-server;

– proksi-server (ishlatilayotgan bo‘lsa);

– foydalanuvchining PBX (kommutatsiyalanuvchi ulanishda Internet aloqasi - telefon liniyasi orqali) yoki oxirgi milning boshqa uskunalari (xDSL, Wi-Fi, GPRS va h.k).

Natijada bitta foydalanuvchi harakati - veb-sahifani ko‘rish bilan o‘zaro bog‘liq bo‘lgan yozuvlar saqlanadigan ikki yoki uchta joy to‘planishi mumkin.

Ko‘proq murakkab usullar bilan foydalanuvchi harakatlarining izlari qolishi mumkin bo‘lgan joylar ham ko‘p. Bu joylarning barchasini aniqlash va tegishli loglar uchun kimga murojaat qilish kerakligini aniqlash AT mutaxassisining vazifasidir. Eng ilg‘or tergovchi ham uni o‘rnini bosa olmaydi. Shuning uchun bunday hollarda mutaxassisni jalb qilish majburiydir.

Veb-server loglarini tekshirish. Veb-serverning jurnallarida qanday ma’lumotlarni topish mumkin? Bunday ma’lumotlarning to‘plami veb-server turiga va uning sozlamalariga bog‘liq. Ko‘pincha loglar quyidagi ma’lumotlarni o‘z ichiga oladi:

– mijoz IP-manzili;

– soat mintaqasini o‘z ichiga olgan so‘rov vaqti;

– HTTP mijozi so‘rov maydonlari

– autentifikatsiya mavjud bo‘lsa, foydalanuvchi identifikatori;

– so‘ralgan veb-sahifaning URL manzili va uning individual elementlari (domen, yo‘l, parametr);

– haqiqiy IP (anonim bo‘lmagan proksi-server orqali kirishda)

– mijozlar brauzer identifikatsiya stoli (til va operatsion tizimni o‘z ichiga oladi);

– havola qilish (referrer), ya’ni bu sahifaga havola qilingan veb-sahifaning manzili;

– boshqa joylar to‘g‘risidagi veb-server javobining mazmuni (MIME type);

– veb-server javob kodi (status code);

– veb-serverning javob hajmi (HTTP sarlavhasini tashqari);

– veb-sahifalarga kirish paytida sodir bo‘lgan xatolar.

Loglarga ishonib bo‘ladimi? Veb-serverning loglarida qaysi ma’lumotlar veb-serverga kirish imkoniyatiga ega bo‘lmasdan soxtalashtirilishi mumkin?

Faqat HTTP so‘rov joylari. Ushbu so‘rov mijoz tomonida to‘liq shakllanadi, shuning uchun agar istasa, tajovuzkor har qanday maydonni biron bir qiymat bilan kiritishi mumkin.

Logda saqlangan IP-manzil ishonchli bo‘lishi mumkin. Tabiiyki, bu proksi-server yoki soks-serverining yoki boshqa vositachining IP-si bo‘lishi mumkin, boshqa joylar ham ishonchli bo‘lishi mumkin bo‘lgan veb-serverning ichki ma’lumotlari (javob kodi, sahifa hajmi, va hokazo) bo‘lishi mumkin.

Veb-serverning ma’lumotlar loglarining to‘g‘riligini tekshirish uchun, ular bir-biri bilan bir qatorda boshqa loglar bilan o‘zaro taqqoslanadi. Turli loglarni taqqoslashning foydaliligini namoyish qilib, amaliyotdan misol keltiraylik. Internet-kazinodagi axborot xavfsizligini ta’minlash xizmatining xodimi, veb-serverning loglarini tahlil qilib, HTTP-so‘rovining maydonlariga ko‘ra, o‘yinchilarning brauzeri rus tilini qo‘llab-quvvatlayotganini payqadi. Bunday holatda, IP manzil Koreya uchun berilgan. Koreys tili bo‘yicha yo‘riqnoma yo‘q edi. Bu shubha uyg‘otdi. Xodim boshqa hisobdan foydalanuvchi hisob raqamiga kirganida tekshirildi. Bu bitta IP bilan aniqlandi. Keyin u boshqa foydalanuvchilarning bir xil IP-ga kirishlarini tekshirdi. Bu koreysning IP-manzilini hech kim ishlatmagan. Ammo xavfsizlik xizmati xodimi tinchlanmadi va bir xil sozlamalardagi boshqa so‘rovlar ushbu manzilga yetib kelganligini tekshiradi. Xuddi shu brauzerda 10dan ortiq hisob qaydnomasi qayd etilgan. Bu foydalanuvchilar turli davlatlarning IP manzillaridan kelib tushdi va mamlakat foydalanuvchi nomiga mos keldi. Biroq bu foydalanuvchilarning barchasi uchun (shu jumladan, rus tilini qo‘llab-quvvatlashni ham o‘z ichiga olgan) brauzer sozlamalari to‘plami

katta shubha uyg‘otdi. Xodimning barcha shubhali foydalanuvchilarning faoliyat davrlarini taqqoslaganda, ular bir-biri bilan kesishmasligini va, shuningdek, bir-biriga qo‘shilishlarini ko‘rdilar. U turli mamlakatlardagi ***soks-serverlarini*** ishlatib, o‘g‘irlangan kartochkalarni hisobga olgan holda, u bilan hisob-kitob qilish bilan shug‘ullanayotgan karderga duch kelganini tushundi. Keyingi tekshiruvlar buni tasdiqlangan.

Tizim loglarini tadqiq qilish. Operatsion tizimda hodisalarni ro‘yxatga olish xavfsizlikning uchta komponentidan biridir. Bu **"AAA"** modeli - **authentication, authorization, accounting - autentifikatsiya qilish, avtorizatsiya qilish, audit.** Tizim xavfsizligiga bevosita yoki bilvosita aloqador bo‘lgan barcha hodisalarni qayd qilish auditning mohiyatini tashkil etadi. O‘ziga logotip qo‘yish buzg‘unchiga axborot tizimiga ruxsatsiz kirishini taqiqlamaydi. Shu bilan birga, bu uning aniqlanish ehtimoli, shuningdek, tajovuzkorning keyingi topilishi va ta’sirini kuchaytiradi. Bundan tashqari, jurnallar himoyalangan tizimning zaifliklarini aniqlashga yordam beradi.

Audit qanchalik kengroq bo‘lsa, kompyuter jinoyatlarini tergov qilish shunchalik osonlashadi. Saqlangan ma’lumotlardan foydalanib, mutaxassis ish uchun ko‘plab foydali ma’lumotlarni olishlari mumkin.

Operatsion tizimlarning turli sinflari uchun qurilma tizimidagi audit voqealarini ko‘rib chiqaymiz.

Windows tizimi loglari. Windows operatsion tizimlarida uchta loglar mavjud: dastur loglari (application log), tizim loglari (system log) va xavfsizlik loglari (security log).

Application log da ilova dasturlari va ba’zi xizmatlar tomonidan yaratilgan xabarlar va hodisalar bayon etilgan. System log da operatsion tizim yadrosining voqealarini va eng muhim xizmatlarni o‘z ichiga oladi. Xavfsizlik jurnalida shuningdek, kuzatilgan foydalanuvchilar faoliyati bilan bog‘liq tizim xizmatlari tomonidan ishlab chiqarilgan hodisalar, ularning autentifikatsiyasi va avtorizatsiya qilinishi qayd etiladi. Kompyuterda DNS-server kabi qo‘shimcha dasturlar ishlayotgan bo‘lsa, ushbu uchta logga qo‘shimcha qo‘shish mumkin.

Odatiy rejimda juda kam sonli hodisalar ro‘yxatga olinadi va security log da esa bundaylar umuman yo‘q. Jurnallarda batafsil ma’lumot olish uchun ma’mur ochiq-oydin auditoriyani yoqishi va audit siyosatini sozlashi kerak.

Barcha Windows loglari «Administrative Tools» yoki «Management Console» menyusida joylashgan «Event Viewer» maxsus dasturi tomonidan ko‘rib chiqiladi.

Qidirayotgan narsalarga qarab, tekshirilayotgan kompyuterning "buzish" izlari yoki noqonuniy foydalanuvchi faoliyatining izlari, turli loglardan olingan turli ma’lumot foydali bo‘lishi mumkin.

UNIX va Linux tizim jurnallari. UNIX operatsion tizimlarning xilma-xilligiga qaramay, ularning barchasi tizim jurnallarini yig‘ish va saqlash uchun o‘xshash tizimga ega. «MacOS-X» operatsion tizimida hodisalarni loglarga yozish xuddi shunday tarzda joylashtirilgan.

Syslogd deb ataladigan maxsus dastur (jarayonlar) turli dasturlar va jarayonlardan xabarlar oladi va ularni tegishli fayllarga aylantiradi. Bir manbadan xabarlar turli fayllarga yuborilishi mumkin, turli manbalardan xabarlar bir xil faylga yuborilishi mumkin - tizim juda moslashuvchan tarzda tuzilgan. Voqealar xabarlari mahalliy yoki tarmoq orqali qabul qilinadi/ Har ikkala usul ham bir xil protokoldan foydalanadi.

Yaratilgan har bir xabar ikkita identifikatsiyalash xususiyatiga ega - ustuvor (priority) va resurs (facility). Ularning birikmasi fayllar tomonidan olingan xabarlarni keyinroq tartiblash uchun xizmat qiladi.

Qabul qilingan syslogd xabarlari vaqt tamg‘asi bilan ta’minlangan va bitta xabar asosida bitta matn bo‘yicha tekis matnli faylga yoziladi. Ushbu xabarlarni matnli fayllar bilan ishlaydigan har qanday matn muharriri yoki boshqa dasturda ko‘rish mumkin.

IOS tizim loglari. Internetdagi kalit va routerlarning sezilarli qismi (agar ko‘pi bo‘lmasa) IOS operatsion tizimini boshqaradi. Aloqa asboblari uchun boshqa operatsion tizimlari OTga o‘xshash, xususan, ular xuddi shu tarzda tizimga kirishadi. Bunday odatiy qurilmalar orasida «Cisco», «Juniper», «Huawei» va boshqa bir qator brendlar bilan jihozlangan kommunikatsiya uskunalari mavjud. Bu ko‘pchilikni tashkil etadi.

IOS tizimida quyidagi hodisalar qayd qilinadi:

– interfeysi yoki port maqomini o‘zgartirish;
– ma’mur yoki qurilma ruxsati;
– qurilma konfiguratsiyasini o‘zgartirish va saqlash;
– (ACL entry) qoidasiga mos tushuvchi tranzit paketini qabul qilishi;
– boshqalar.

Voqealar xabarlari odatda syslog yoki SNMP orqali tashqi log serveriga yuboriladi. Bundan tashqari, bir nechta so‘nggi xabarlar tezkor

xotira buferida saqlanadi va tegishli buyruq (show logging) bilan koʻrsatilishi mumkin.

Agar aloqa asbob-uskunalari loglari bilan tanishish kerak boʻlsa, quyidagilarni qilish kerak:

– ushbu qurilma qayerdan yuborilganligini aniqlash uchun mavjud qurilma konfiguratsiyasiga (konfiguratsiya fayli) kirish huquqini beradi (show running-config buyrugʻi); yuqorida koʻrsatilgan konfiguratsiyani (yoki faqat loglarga tegishli qismini) saqlash va hujjatlashtirish;

– (ixtiyoriy) soʻnggi xabarlar bilan qurilma buferini koʻrish;

– roʻyxatga oluvchi serverni, ya'ni loglarni qabul qiladigan va saqlaydigan serverni aniqlash;

– roʻyxatga oluvchi serverga kirish huquqini qoʻlga kiritish va qiziqtiradigan qurilmadan olingan loglarning qaysi faylga kiritilishini aniqlash uchun uning syslog- demoni konfiguratsiyasi bilan tanishish; yuqoridagi syslog-demon konfiguratsiyasini saqlash va hujjatlashtirish;

– kerakli qurilmadan jurnallar saqlangan fayllarni tekshirish yoki oʻchirish.

– Ozchilikni tashkil etuvchi ba'zi aloqa qurilmalari IOS va shunga oʻxshashlarni ishlatmaydi. Bunday notabiiy qurilmalarda loglarni boshqacha tartibda ajratish mumkin. Ayniqsa, loglar lokal ravishda saqlanishi yoki nostandart protokol yordamida roʻyxatga olish serveriga uzatilishi mumkin.

3.7. Keyloggerlar

Keylogger (inglizcha ***keylogger, key*** **- klavisha va** ***logger*** **- yozish qurilmasi**) - har xil foydalanuvchi harakatlarini - kompyuter klaviaturasida bosish, harakat va sichqonchani bosishni yozib olgan dasturiy ta'minot yoki apparat.

Tekshirilishi mumkin boʻlgan axborot turlari:

– klaviaturada tugmalarining bosilishi;

– sichqonchaning harakati va bosilishi;

– bosilish sanasi va vaqti.

Qoʻshimcha sifatida, ba'zi hollarda davriy ekran suratlari amalga oshirilishi (va ba'zi hollarda - hatto video ekran) va buferdan ma'lumotlar nusxasi koʻchirilishi mumkin.

Keylogger, kompyuter klaviaturasi bilan barcha manipulyatsiyani aniqlab, ro‘yxatga oluvchi har qanday dasturiy ta’minot yoki apparatning tarkibiy qismidir. Ko‘pincha keylogger klaviatura va operatsion tizim o‘rtasida joylashgan va barcha foydalanuvchilar harakatlarini qo‘lga kiritadi. Ushbu vosita yoki olingan ma’lumotlarni quvvatlangan kompyuterda saqlaydi, yoki u katta hujumning bir qismi bo‘lsa, barcha ma’lumotlar darhol hujum uyushtirgan tashkilotlarning uzoq kompyuteriga uzatiladi.

Keylogger tasnifi.

Dastur keyloggerlari shaxsiy kompyuter foydalanuvchilari faoliyati ustidan nazoratni amalga oshiradigan dasturiy mahsulotlar guruhiga kiradi.

Dastlab, ushbu turdagi dastur faqat klaviaturada tugmachalar, jumladan, tizim tugmachalari haqida ma’lumotni maxsus jurnalga yozib olish uchun mo‘ljallangan (log-fayl), keyinchalik ushbu jurnal dasturni o‘rnatgan shaxs tomonidan o‘rgangan. Log fayl tarmoq orqali tarmoq diskiga, FTP-serveriga, Internetda e-pochta va hokazoga yuborilishi mumkin.

Ayni paytda dasturiy ta’minot ko‘pgina qo‘shimcha vazifalarni amalga oshiradi - bularga oynalardan, sichqoncha bosilishlaridan va buferdan ma’lumotni ushlab qolish, ekran va aktiv zonalarning suratlarini hosil qilish, yuborilgan va qabul qilingan e-mail larning ro‘yxatini yuritish, tizim reestori bilan yuritilgan ish va fayl aktivligini kuzatish, printerga yuborilgan topshiriqlarni yozib olish, kompyuterga ulangan mikrofondan ovozni hamda kameradan suratlarni qo‘lga kiritish kiradi.

Apparat keyloggerlari klaviatura va kompyuter o‘rtasida biriktirilishi mumkin bo‘lgan yoki klaviaturaning o‘zida joylashgan kichik qurilmalardir. U klaviaturada tugmachalarning barcha bosilishlarini yozib oladi. Ro‘yxatga olish jarayoni oxirgi foydalanuvchiga to‘liq ko‘rinmaydi. Apparat keylogerlari barcha tugmachalarni muvaffaqiyatli ushlab turish uchun kompyuterda biron-bir dasturni o‘rnatishni talab qilmaydi. Uning ish vaqti cheklanmagan, chunki uning ishi uchun qo‘shimcha quvvat manbai talab qilinmaydi.

Ushbu qurilmalarning ichki uzluksiz xotirasi hajmi 20 millionga yaqin klaviatura bosilishlarini saqlash imkonini beradi. Ushbu qurilmalar har qanday shaklda ishlab chiqarilishi mumkin, shuning uchun ham mutaxassis, ba’zida axborotni boshqarish paytida o‘zlarining

mavjudligini aniqlay olmaydi. Ulanish joyiga qarab apparat keyloggerlari tashqi va ichki bo‘linadi.

Dasturiy ta’minot keyloggerlariga qaytaylik. Keyloggerlarning bu oilasi juda xilma-xildir va ko‘pincha ma’lum bir turi professional xakerlar tomonidan muayyan vazifani bajarish uchun bitta variantda ishlab chiqarilishi mumkin. Bundan tashqari, antivirusdan yashirish juda oson ekanligi ularni shaxsiy ma’lumotlar uchun juda xavfli qiladi.

Akustik keyloggerlar - bu kompyuter klaviaturasi tugmachalari bosilganda foydalanuvchi tomonidan yaratilgan tovushlarni birinchi marta qayd etadigan apparat qurilmalari bo‘lib, u keyin bu tovushlarni tahlil qiladi va matn formatiga aylantiradi.

Dasturli keyloggerlar ko‘pincha murakkab zararli dasturlarning bir qismi sifatida o‘rnatiladi. Virusli saytga tashrif buyurilganda maqsadli kompyuterlarga maxfiy yuklanish vaqtida virus o‘rnatilishi mumkin.

Ko‘pincha, keyloggerlar turli yo‘llar bilan va turli bahonalar ostida to‘liq huquqiy dasturiy ta’minot o‘rnatilgan bo‘lishi mumkin. Uskuna keyloggerlari kompyuterga jismoniy kirish imkoniga ega bo‘lgan tajovuzkor tomonidan o‘rnatiladi.

Aniqlash va olib tashlash. Zararli keyloggerlarni aniqlash juda qiyin, chunki ular har doim ham boshqa ko‘plab zararli dasturlarga o‘xshamaydi. Ular qimmatli ma’lumotni izlamaydilar va uni uzoq serverga yubormaydilar, ular viruslangan qurilmada ma’lumotlarni yo‘q qilishga harakat qilmaydi. Keyloggerlar o‘z ishini jim va sezdirmasdan bajaradilar. Antivirus dasturlari barcha ma’lum keyloggerlar turlarini ko‘rish, aniqlash va yo‘q qilish imkoniyatiga ega. Biroq muayyan foydalanuvchilarga qarshi hujumni amalga oshirishga mo‘ljallangan keyloggerlarni aniqlash oson emas, chunki ular ko‘pincha ma’lum zararli dastur sifatida ro‘yxatdan o‘tmagan. Shunga qaramay, ertami-kechmi, ular uzatilgan serverga ruxsatsiz ma’lumotlarni yuborish orqali o‘zlarini namoyon qila boshlagach aniqlanadi.

Keyloggerlardan himoya qilish usullari.

1. Noqonuniy ravishda o‘rnatilgan "ma’lum" ruxsat etilmagan dasturiy ta’minot keyloggerlariga qarshi himoya:

– ma’lumotlar bazalari avtomatik yangilash bilan ishlab chiqaruvchilar;

– ishonchli anti-shpion dasturi va/yoki anti-virus dasturiy mahsulotlardan foydalanish.

2. "Ma’lum bo‘lmagan" ruxsat etilmagan dasturiy ta’minot keyloggerlariga qarshi himoya:

– evrisitk, ya’ni imzo bazasini talab qilmaydigan analizatorlardan shpion dastur mahsulotlariga qarshi kurashda qo‘llaydigan mashhur ishlab chiqaruvchilarning antishpion va/yoki antivirus dasturlaridan foydalanish;

– apparat darajasida bunday shifrlashni, klaviatura ma’lumotlar, shuningdek, klaviaturalar foydalanishlarini shifrlash dasturlaridan foydalanish.

3. «Ma’lum» va «noma’lum» dasturiy ta’minot dasturlar keyloglaridan himoya qilish taniqli ishlab chiqaruvchilarning antishpion dasturiy ta’minot va/yoki virusga qarshi dasturiy ta’minot mahsulotlaridan foydalanishni o‘z ichiga oladi. Bunday ta’minotlar quyidagilardan iborat:

– doimiy yangilanadigan shpion dasturlarining imzo ma’lumotlar bazasi;

– imzo ma’lumotlar bazasini talab qilmaydigan evristik (xulq-atvor) analizatorlari.

4. Ruxsatsiz o‘rnatilgan apparat keyloggerlaridan himoyalanish:

– kompyuter tizimlarining puxta tashqi va ichki kuzatuvi;

– virtual klaviaturalar foydalanish.

3.8. Trafikni qo‘lga kiritish va tadqiq qilish

Trafikni qo‘lga kiritish quyidagi yo‘llarda amalga oshirilishi mumkin:

– o‘rniga interfeysni oddiy usulda “eshitish” usulida (ushbu usul kommutatorlar (svitchlar) o‘rniga segmentlarda konsentratorlar (xablardan) foydalanilganda samaralidir, aks holda u samara bermaydi, negaki sniferga faqatgina alohida freymlar tushadi);

– kanalning uzilishiga snifferni ulash;

– trafikni bo‘lish (dasturiy ta’minot yoki apparat) va uni snifferga yuborish;

– soxta elektromagnit nurlanishni tahlil qilish va shu orqali trafikni tiklash;

– kanal (MAC- spoofing) yoki tarmoq(IP- spoofing) darajasida hujum orqali.

Hujum jabrlanuvchi trafigini yoki segmentning to‘liq trafigini sniferga yuborish va keyinchalik kerakli manzilga qaytarishga olib keladi.

"**Sniffer**" atamasi inglizcha "**to sniff**" so‘zidan olingan bo‘lib **"hidlash"** degan ma’noni bildiradi - tarmoq yoki faqat boshqa tugunlar uchun mo‘ljallangan trafikni qo‘lga kiritish va tahlillash yoki faqat tahlillash uchun mo‘ljallangan vositalar.

Snifferlar ham yaxshi, ham yomon maqsadlarda ishlatiladi. Sniffer orqali o‘tgan trafikni tahlil qilish quyidagi imkoniyatlarni beradi:

– virusli va zararli trafikni aniqlash, uning mavjudligi tarmoq uskunalari va aloqa kanallarining yukini oshiradi (bu yerda snifferlar samarasiz, odatda serverlar tomonidan turli statistika to‘plash va faol tarmoq asbob-uskunalari va undan keyingi tahlillar qo‘llaniladi);

– tarmoqdagi zararli va ruxsatsiz DTni , masalan, tarmoq skanerlari, fluderlarni, troyan otlari, piring mijozlari va boshqalarni aniqlash (bu odatda maxsus sniferlar - tarmoq faoliyati monitoring qiluvchi vositalar yordamida amalga oshiriladi);

– parol va boshqa ma’lumotlarni olish maqsadida har qanday shifrlanmagan (va ba’zan shifrlangan) foydalanuvchi trafigini qo‘lga olish;

– tarmoq nosozligi yoki tarmoq agentlari sozlamalaridagi xatoni lokallashtirish (ushbu maqsad uchun tizim ma’murlari ko‘pincha sniferlardan foydalanishadi).

Wireshark - tarmoq trafigi analizatori. Uning vazifasi tarmoq trafigining qo‘lga kiritish va uni batafsil ko‘rsatish. Tarmoqli transport analizatorini elektr kabelida nima sodir bo‘lishini ko‘rish uchun ishlatiladigan o‘lchash qurilmasi bilan taqqoslash mumkin, masalan, elektrenergiya xodimlarining elektr kabelida nima sodir bo‘lishini aniqlash uchun foydalanadigan voltmetr (lekin, albatta, yuqori darajadagi). O‘tmishda bunday vositalar juda qimmat bo‘lgan. Biroq Wireshark kabi bir vosita paydo bo‘lganidan beri vaziyat o‘zgargan.

Wireshark, bugungi kunda mavjud bo‘lgan eng yaxshi tarmoq trafigi analizatorlaridan biridir. Wireshark Pcap kutubxonasiga asoslangan. Kutubxona Pcap (Packet Capture) kompyuterning tarmoq interfeysi kartasiga kelgan tarmoq ma’lumotlarini tahlil qilish uchun dasturlarni yaratishga imkon beradi.

Tarmoqni monitoring qilish va sinovdan o‘tkazishning turli xil dasturlari, sniferlar ushbu kutubxonadan foydalanadilar. U C/C++ tilida yozilgan, shunday ekan Java, .NET va skript tillaridan foydalanish oqilona emas. Unix kabi tizimlar uchun libpcap kutubxonasi ishlatiladi va Microsoft Windows uchun WinPcap kutubxonasi ishlatiladi.

Tarmoqni monitoring qilish dasturi libpcap yoki WinPcap-dan tarmoq bo‘ylab harakat qilgan paketlarni qo‘lga kiritish uchun va yangi versiyalarda tarmoqdagi paketlarni uzatish uchun foydalanilishi mumkin. Libpcap i WinPcap shuningdek, olingan paketlarni faylga saqlashni va saqlangan paketlarni o‘z ichiga olgan fayllarni o‘qishni qo‘llab-quvvatlaydi.

libpcap yoki WinPcap asosida tuzilgan dasturlar tarmoq trafigini egallashi va tahlil qilishi mumkin. Qabul qilingan trafik fayli Pcap ni ishlatadigan ilovalar uchun tushunarli bo‘lgan formatda saqlanadi.

Wireshark nima uchun ishlatiladi?

– Tizim ma’muri tarmoqdagi muammolarni hal qilish uchun uni ishlatadi.

– Xavfsizlik auditorlari tarmoq muammolarini aniqlash uchun foydalanadilar.

– Ishlab chiqaruvchilar tarmoq ilovalarini tuzatish uchun foydalanadilar.

– Muntazam foydalanuvchilar ushbu vositadan tarmoq protokollari ichki strukturasini o‘rganish uchun foydalanadilar.

Wireshark xususiyatlari :

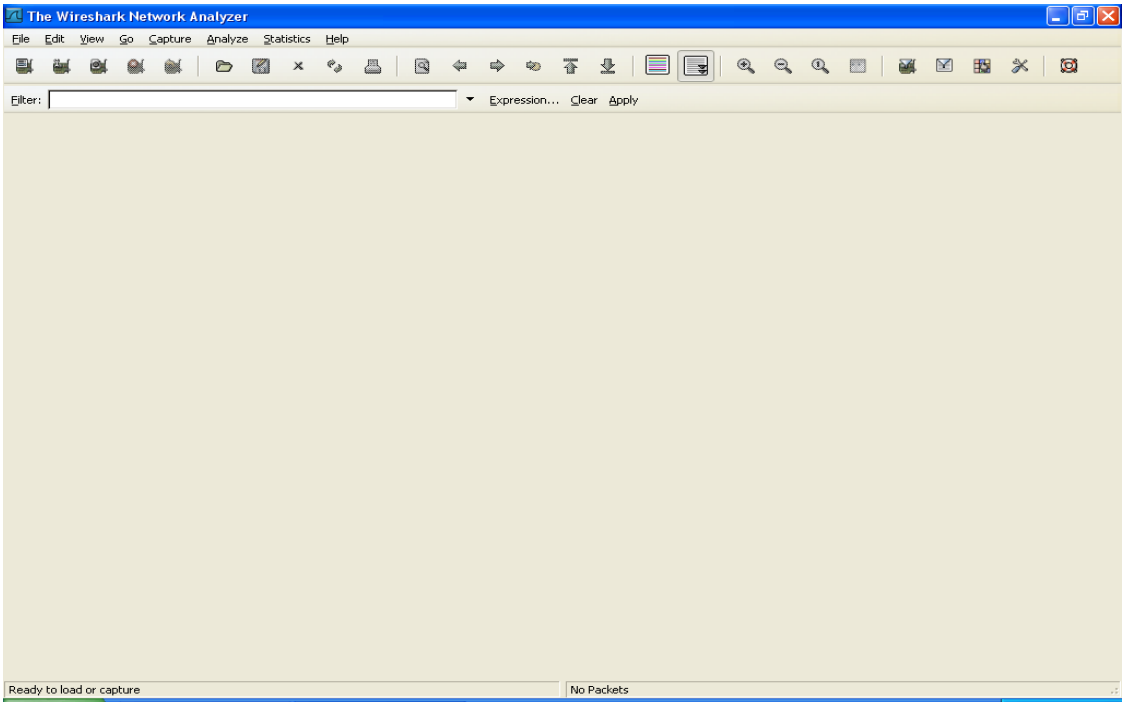
1. Eng zamonaviy operatsion tizimlarida ishlaydi (Microsoft Windows, Mac OS X, UNIX).
2. Haqiqiy vaqtda tarmoq interfeysi trafigini qo‘lga kiritadi. Wireshark, turli xil tarmoq qurilmalarida trafikni qo‘lga kiritishi va nomini (jumladan, simsiz qurilmalar) ko‘rsatishi mumkin.
3. Protokol dekoderlarining ko‘pligi (TELNET, FTP, POP, RLOGIN, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, MSN, YMSG va boshqalar).
4. Oldindan saqlangan tarmoq trafigini saqlaydi va ochadi.
5. Paketlarni bir necha mezonlarga ko‘ra filtrlashga ruxsat beradi.
6. Paketlarni turli mezonlarga qarab qidirishga ruxsat beradi.
7. Turli xil protokollarning olingan paketlarini yoritish imkonini beradi.
8. Turli xil statistika yaratishga imkon beradi.

Wireshark - bu hujumni aniqlash tizimi emas. Tarmoqdagi biron kimsa shubhali ishlarni amalga oshirsa, u ogohlantirmaydi. Biroq agar bu ro‘y berayotgan bo‘lsa, Wireshark haqiqatan yuz berganligini

tushunishga yordam beradi. Wireshark tarmoq trafigini qanday yaratishni bilmaydi, u faqat mavjud bo‘lganlarni tahlil qiladi.

Wireshark interfeysi

Wireshark dastur interfeysi 13- rasmda ko‘rsatilgan .



13- rasm. Wireshark dasturining asosiy oynasi

Yuqorida joylashganlar Windows ilovalari menyusi va asboblar paneli uchun standart bo‘lib, ular haqida to‘xtalib o‘tirishga xojat yo‘q. Keyingi o‘rinda filtr keladi, unda paketni filtrlash sozlamalarini kiritish mumkin. Navbatdagisi olingan barcha paketlar ro‘yxati mavjud oynadir.

Paket raqami, paketni qabul qilishning nisbiy vaqti (hisoblash birinchi paketdan yuritiladi, vaqt ko‘rsatkichlari parametrlari o‘zgarishi mumkin), jo‘natuvchining IP-manzili, qabul qiluvchining IP-manzili, paket orqali jo‘natilgan protokol kabi ma’lumotlarni va shuningdek, turli ranglarda turli xil protokollar yoritiladi, bu aniqlik kiritadi va tahlilni osonlashtiradi.

Keyinchalik, paket haqida batafsil ma’lumot OSI tarmoq modeli bo‘yicha taqdim etilgan oynani ko‘rish mumkin. Nihoyat, eng pastki oynada HEX formatdagi paket, bayt bo‘yicha ko‘rsatiladi. Interfeys konfiguratsiyasi View menyusida osongina o‘zgartirilishi mumkin.

Misol uchun, ko‘p holatlarda (paketdagi ma’lumotlarni tahlil qilish bundan mustasno), u zaruriy emas va batafsil tavsiflovchi oynadan

ma’lumotlarni takrorlashi sababli, paketni bayt ko‘rsatuvchi oyna olib tashlanishi mumkin (u ham View menyusidagi Paket baytidir).

Trafikni qo‘lga kiritish - Wiresharkning asosiy xususiyatlaridan biridir. Wireshark qo‘ga kiritish mexanizmi quyidagi xususiyatlarni taqdim etadi:

– turli xil tarmoq uskunalari (Ethernet, Token Ring, ATM va hokazo) trafikini ushlash;

– turli xil voqealar asosida qo‘lga olish: qo‘lga olingan ma’lumotlar hajmi, ushlab olish muddati, paketlar soni;

– qo‘lga kiritish vaqtida dekodlangan paketlarni ko‘rsatish;

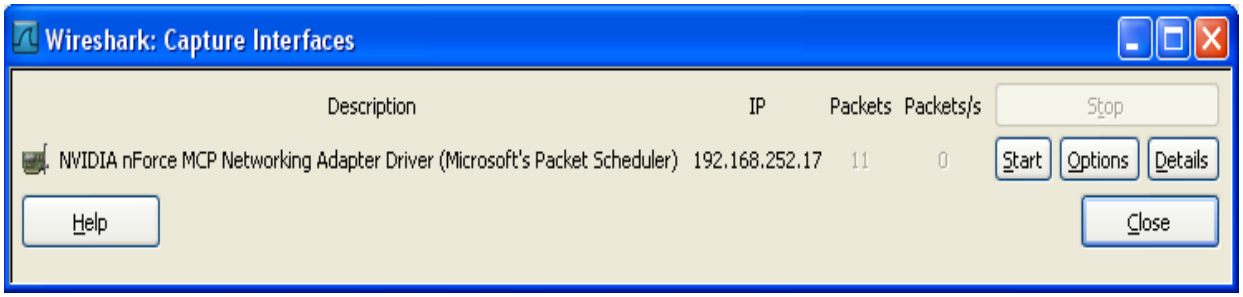
– ushlangan axborotning hajmini kamaytirish uchun paketli filtrlash;

– agar qo‘lga olish ko‘p vaqt davom etsa, bir nechta fayllarni yozib olish.

Traffikni qo‘lga olishni boshlash uchun ushbu tizimda Ma’mur huquqlariga ega bo‘lish va to‘g‘ri tarmoq interfeysini tanlash kerak. Ta’qib qilishni amalga oshiradigan tarmoq adapterini tanlash uchun asboblar panelidagi Interfaces tugmasini yoki Capture > Interfaces menyusiga bosish kerak .

Bu tugmalar biri bosgan keyin oyna tizimida mavjud tarmoq interfeysi ro‘yxati paydo bo‘ladi (14- rasm).

14- rasm. Tarmoq interfeyslari ro‘yxati



Ushbu ro‘yxatda interfeys nomi, interfeysning IP-manzili, interfeysning tarmoq faoliyati (oyna paydo bo‘lganidan boshlab paketlarning umumiy soni va soniyada paketlarning soni sifatida ko‘rsatilgan) kabi ma’lumotlar ko‘rsatiladi. Bundan tashqari, ushbu oynada interfeys haqidagi ma’lumotlar ham mavjud.

Qo‘llash qoidalarida paketlarni filtrlash, bir qator fayllarga yozib qo‘yish, turli me’zonlar (paketlar soni, megabayt soni, daqiqalar soni), paketlarni ko‘rsatish variantlarini o‘zgartirish mumkin. Ko‘pgina

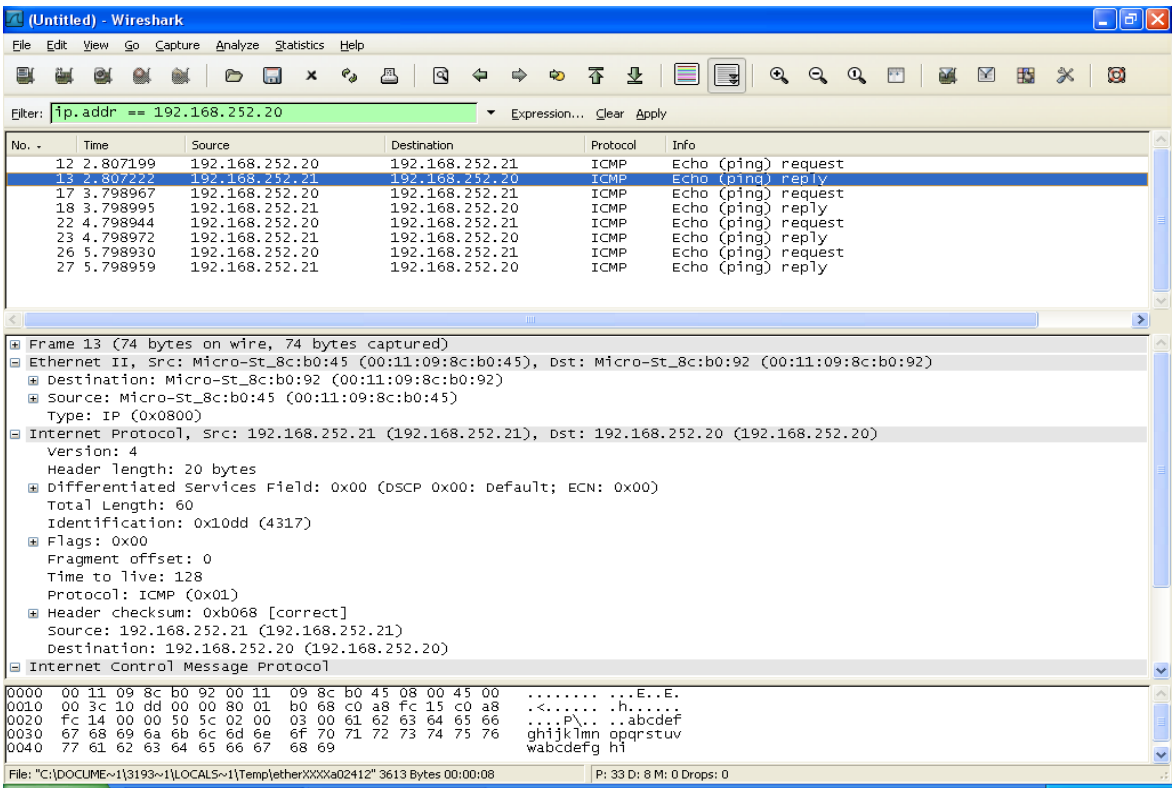
hollarda, bu parametrlar standart sifatida qoldiriladi. Shunday qilib, hamma narsa trafikni qo‘lga kiritishga tayyor, "Start" tugmasini bosish kerak.

Start tugmasini bosgandan so‘ng, paketni qo‘lga olish boshlandi. Tarmoq faoliyati yuqori bo‘lsa, unda darhol kiruvchi yoki chiquvchi ko‘plab paketlarni ko‘rish mumkin. Endilikda taniqli ping dasturini o‘rganaylik.

Ping utilitasi.

Win + R ni bosamiz va qatorga cmd kiritamiz. Konsol ochiladi, u yerda ping <IP manzil> buyrug‘ini kiritamiz. IP-manzili ma’lum bir tarmoq konfiguratsiyasiga asosan yozilishi kerak. Endi, agar xost xali muvaffaqiyatli tarzda so‘ralgan bo‘lsa, Wireshark oynasini batafsilroq ko‘rib chiqish uchun ochamiz. Bu yerda qiyinchiliklarni ko‘ramiz va buni tushunish uchun uzoq vaqt talab qilinadi. Bu yerda filtrlar bizga yordamga keladi.

Ping utiliti dasturi ICMP protokoli bo‘yicha ishlaydi, shuning uchun biz ushbu protokolning nomini filtr qatoriga kiritamiz va Apply ni bosamiz. 15- rasmga o‘xshash natija hosil bo‘lishi kerak. Bu yerda ICMP protokoli ichida Echo request va Echo Reply qanday amalga oshishini: qanday sinov ma’lumotlar yuborilayotganini, aynan qaysi bayroqchalar bu Echo request ni anglatishini va boshqa muhim axborotlarni ko‘rishimiz mumkin.



15- rasm. ICMP protokoli bo‘yicha filtrlash

FTP trafigini qo‘lga kiritish. Ushbu punktda, FTP protokoli orqali shifrlanmasdan uzatiladigan hujjatning saqlanishi ko‘rib chiqiladi va TLS ga asoslangan shifrlashdan foydalanilganda foydali bo‘lgan narsalarni qo‘lga kiritib bo‘lmaslikka ishonch hosil qilamiz. Cerberus FTP Server FTP server sifatida ishlatiladi va har qanday brauzer masalan, Internet Explorer mijoz sifatida ishlatiladi (bu ishda FireFTP deb nomlangan Mozilla Firefox plagini qo‘llaniladi).

Wireshark da paketni qo‘lga kiritish boshlanadi va qulaylik uchun FTP orqali filtrlash o‘tkaziladi (“ftp or ftp-data” qo‘shtirnoqsiz teriladi). FTP serveri manzili brauzerning manzil satriga kiritiladi: ftp://<server IP manzili> va Enter tugmasi bosiladi. Serverda test.txt deb nomlangan matn hujjati bo‘ladi, u yuklab olinadi. Endi esa sniferda nima sodir bo‘lganini va qanday paketlar qo‘lga kiritilganini ko‘rib chiqamiz. Faqatgina ma’lumotni emas, balki login va parolni ham qo‘lga olish mumkin. Shunday qilib biz ushlangan paketlarda hujjatning mazmunini topamiz. FTP fayllarini uzatish jarayoni haqida bir necha so‘z: server avval mijozga qutlov bannerini (bu holda, 220-Welcome to Cerberus FTP Server) yuboradi, foydalanuvchi USER va PASS komandalaridan foydalangan holda serverda tasdiqlanadi, buyruqni ishlatadigan katalog ro‘yxati LIST va RETR buyrug‘i yordamida kerakli faylni suratga oladi. RETR buyrug‘ini paketlar ro‘yxatida izlaymiz. Buni amalga oshirish uchun Ctrl+F tugmasini bosib, qidiruv parametrlarida Find by String va Search in Packet Bytes tanlanadi, qidiruv maydonchasida RETR kiritiladi va Enter tugmasini bosiladi. Agar fayl mavjud bo‘lsa, mijoz serverga buyruq yuborgan paket topiladi, server 150 Opening data connection javobini, keyinchalik esa hujjat mazmuni saqlanuvchi paketni yuboradi. Snifing muammosi avvalroq - xablarga asoslangan tarmoqlarda dolzarb bo‘lgan - bu svitchlar tarmoqlari uchun ARP spoofing texnologiyasi tufayli hozir ham dolzarb bo‘lib qolmoqda. Bundan tashqari, bugungi kunda passiv rejimdagi sniffing amalga oshirilishi mumkin bo‘lgan simsiz tarmoq jadal sur’atlarda rivojlanib bormoqda.

Snifingni oldini olishda yagona yechim shifrlashdir. Ma’lumotni ishonchli bo‘lmagan dastur protokollari yoki eski protokollar orqali ochiqdan-ochiq yetkazib berilishiga yo‘l qo‘ymang. Xavfsiz bo‘lmagan protokollarni (masalan, SSH) shifrlangan ishonchli protokollarga (masalan, telnet) qo‘lga olish uchun jiddiy to‘siqni yaratadi. Ko‘p hollarda barcha xavfli protokollarni almashtirish mumkin emas.

3.9. Kompyuter jinoyatlarini fosh etish xususiyatlari

Kompyuter jinoyatchilarini (xakerlarni) aniqlash uchun quyidagilar kerak:

– nazorat uchun dasturiy ta’minot;
– jurnallarni muntazam tekshirish tizimi;
– "kuzatuv" tizimi.

Dasturiy ta’minot ish jarayonidaligini hisobga olib, jinoyatning eng aniq izlari ikki qismga bo‘linishi mumkin: ***tashqi va ichki.***

Aloqa tizimiga kirish bilan bog‘liq **tashqi izlar**:

– aloqa kabellari va signal qurilmalarining ishdan chiqishi;
– optik aloqa liniyalarida signallarning susayishini kuchaytirish;
– kuchlanish, sig‘im, qarshilik yoki chastotadagi o‘zgarishlar.

Oddiy kirish usuli yoki uzoq masofa orqali kirishga urinish bilan bog‘liq **ichki izlar** quyidagilar:

– turli davomiylikdagi telefon qo‘ng‘iroqlari. Ulardan so‘ng odatda modem tovushini eshitish mumkin. Bu diskning ketma-ket avtomatik terilishi orqali sodir bo‘lgan hujumdan dalolat beradi;
– muvaffaqiyatsiz kirishga urinishlar sonining qaytarilishi;
– boshqarish komandalarini uzatishni takrorlash;
– ruxsatsiz yoki rejalashtirilmagan ish;
– haqoratli yoki shafqatsiz xabarlar;
– yo‘q qilingan yoki buzilgan axborot;
– ko‘chirilgan yoki o‘zgartirilgan fayllar va yangi yaratilgan kataloglar;
– mijozlardan, yetkazib beruvchilardan va foydalanuvchilardan tizimdagi kirish va ish yuritishda tasodifiy xatolar va qiyinchiliklar haqida shikoyat.

Tashkilot xakerdan kamida bir qadam oldinda harakat qilishi kerak. Boshlang‘ich jinoyatchiga oid ma’lumotlar, masalan, quyidagilar orqali to‘planishi mumkin:

– mahalliy pochta qutisiga murojaat qilish va bu orqali buzg‘unchi bo‘limidagi firma to‘g‘risida ma’lumot mavjudligini tekshirish;
– bezovtalangan yoki xavotirga tushgan xodimlarning muammolari bilan shug‘ullanadigan kadrlar bo‘limi bilan aloqada bo‘lish;

– boshqa xakerlarni ushbu kompaniyalar tizimining tafsilotlari bilan tanishtirmasdan, masalan, uchinchi shaxslar orqali ma’lumot beruvchi sifatida ishlatish.

Sanoat josuslari yoki professional xakerlarning potensial faoliyatlarini aniqlash uchun firma turli xil usullarni qo‘llashi kerak:

– masalan, eksport qilish uchun tayyorlab chiqdi sumkalar qaratilgan yashirin kamera yordamida o‘g‘rilikka harakatlarni aniqlash mumkin;

– barcha tashrif buyuruvchilarning, xususan, aloqa bo‘yicha mutaxassislar, elektriklar, suv quvurlari ustalari hamda savdo agentlarining ishonchliligiga amin bo‘lish.

Ayniqsa, xavfli joylar sirasida ijaraga olingan binolar bo‘lib, u yerda kun davomida ko‘pincha asosiy kommunikatsiya markazidan foydalanishni istaydigan 10-15 turdagi mutaxassislarni ko‘rish mumkin. Bunday holda, shaxsiy guvohnomalar kamdan-kam hollarda tekshiriladi. Ma’lumki, binolardagi koridorlar va o‘tish jarayonlari mutaxassislar tomonidan ruxsat etilmagan shaxslarning binolariga olib boriladi.

Mutaxassislar fotosurat va hujjat bilan shaxsning qanday ishlashini ko‘rsatadigan standart identifikatsiya kartasini taqdim etishlari kerak.

Doim oldindan tayyorlangan shifrni yoki rad qilingan xabar kodini telefon orqali tekshirish kerak. Mutaxassis kirish kodini asosiy aloqa tuguniga yozishni talab qilishi kerak, jurnalda quyidagilarni qayd etish lozim:

– tashrif buyurish sanasi va vaqti;
– familiyasi, ismi;
– ish amalga oshirilgan kompaniya nomini;
– identifikatsiya kartasi tekshirilgani fakti.

Ro‘yxatga olish jurnalini vaqti-vaqti bilan tekshirish kerak, barcha tashrif buyuruvchilarni aniqlash kerak. Agar tashrif buyuruvchi xaridor yoki marketing mutaxassisi bo‘lsa, u firma tasdiqnomasi va telefon raqamni ko‘rsatishi lozim, shu yo‘l bilan keyinchalik u haqida ma’lumot olish imkoni bo‘ladi. Shtat qaysi tashrif buyuruvchilardan ehtiyot bo‘lishi haqida ogohlantirilishi kerak. Shubxali shaxslarga quyidagilar kirishi mumkin:

– binoni ijaraga olgan tashkilotlar ro‘yxatiga kiritilmagan shaxs yoki firma izlayotganliklarini da’vo qilgan ruxsatsiz shaxslar;

– ushbu kompaniya haqida batafsil bilmoqchi bo‘lgan potensial mijozlar, biroq ayni paytda, ularning tashrifi maqsadi- buyurtma to‘g‘risida eslaganda to‘liq ma’lumot bermaydigan shaxslar.

Kotibiyat xodimlari, odatda, ma’lumotsiz ketishga rozi bo‘lmagan shiddatli xaridorni tanish va unga qarshi chora ko‘rishdan xabardor emaslar. Bunday hollarda kotib qat’iyatli bo‘lishi va mehmon kuzatishi yoki yordamchilarni chaqirishi kerak. Biroq bu holatlarda, shubhalar paydo bo‘lishidan avval, ma’lumotlar kotib tomonidan berilib bo‘ladi. Yashirin axborotning tarqalmasligi uchun "toza stollar" siyosati amalga oshirilishi kerak: ish soatlari tugaganidan keyin stol ustida hech qanday hujjatlar qolmasligi kerak va barcha keraksiz qog‘ozlarni savatga solib qo‘yishdan oldin yirtib tashlash kerak.

Tashrif buyuruvchi, so‘rovchi, ishtirokchi va foydalanuvchilarning shikoyatlari taqqoslanishi va tahlil qilinishini amalga oshirishga mos tizim ta’minoti tuzilishi kerak. Bunga quyidagilarga o‘xshash odatiy bo‘lmagan hodisalarni nazorat qiluvchi statistik tahlil paketlari yordam berishi kerak:

– har oqshom bir vaqtning o‘zida tizimlar ishdan chiqadi;
– noto‘g‘ri xabarlar paydo bo‘ladi;
– yetkazishda xatolar kuzatiladi;
– natijalarda farqlar mavjudligi kuzatiladi.

Jinoyatchilik yoki jinoyatni sodir etishda shubhalar paydo bo‘lgandan so‘ng, keng ko‘lamli tergov o‘tkazilishi kerak.

Xakerlar jinoyatlarining oldini olish. Asosiy qoidalarga rioya qilish orqali ko‘plab jinoyatlarga yo‘l qo‘ymaslik mumkin:

– firma kommutatsiya portlarining telefon raqamlarini nashr etmasligi kerak va kommutatsiya tizimidagi sobiq direktorning manziliga ega bo‘lishi kerak;
– ulanish o‘rnatilgandan so‘ng va foydalanuvchi tizimga kirgunga qadar, u hech qanday ma’lumot bermasligi kerak;
– tizim kamida yettita belgidan iborat parollardan foydalanishi kerak, va foydalanuvchi kodlari ishlab chiqaruvchi tomonidan taklif qilinganlardan farq qilishi kerak;
– xodimlar kompaniyadan ishdan bo‘shatilganda doimiy o‘zgarishini kafolatlash uchun dinamik parollarni kiritish dasturi amalga oshirilishi kerak;
– terminal vazifalari aniq belgilangan bo‘lishi kerak, masalan, to‘lov tasdiqlari faqat ma’lum terminallar orqali kiritilishi kerak.

Jinoyatchilar, siyosatchilar, ayg‘oqchi faoliyatni boshqaradigan ekstremistlar ruxsatsiz kirishga yo‘l qo‘ymaslik uchun himoya texnologiyalarini tashkilotning texnologik jarayonlari bilan bog‘lash zarur. Tekshiruv va boshqaruv elementlarining harajatlari xavf darajasiga to‘g‘ri kelishi uchun xavfni baholashni amalga oshirish kerak, bunda boshqaruv va boshqarish harajatlari xavf darajasiga to‘g‘ri kelishi talab qilinadi. Tashkilot tizimdagi jinoyatlarning sabablarini kamaytirishni quyidagi vositalarni amalda qo‘llash orqali erishishi mumkin:

- parollar va shaxsiy identifikatsiyalash protseduralari;
- operatsion tizim ustidan nazorat qilish;
- erkin foydalanishni nazorat qilish;
- ma’lumotlar bazasini nazorat qilish;
- tarmoqni nazorat qilish.

Asosiy xulosalar

Kompyuter jinoyatining oldini olish uni oshkor qilish va tergov qilishdan ancha oson va qulaydir.

Kompyuter jinoyatlarning oldini olish uchun mo‘ljallangan, birgalikda yaxlit tizimini tashkil etuvchi chora-tadbirlarni uch asosiy: huquqiy, tashkiliy, kriminalistik guruhlarga bo‘lish mumkin.

Kompyuter jinoyatlarning katta qismi korxona va tashkilotlarda ma’lumotlarni himoya qilish tashkiliy chora-tadbirlar yetarli emasligi, ruxsatsiz kirishga qarshi himoyaning zaifligi, xodimlarning yetarlicha yo‘riqnomaga ega emasligi tufayli kelib chiqadi.

Domen internetning iyerarxik domen nomining maydonini (filialini) ifodalaydi, bu yagona domen nomi bilan belgilanadi.

Whois termini - server domen yoki IP-manzilini kimning nomiga ro‘yxatdan o‘tgani haqida mijozga ma’lumot yuborishi mumkin bo‘lgan protokol.

Log - bu dasturda saqlanadigan avtomatik voqea jurnali. Odatda har bir voqea jurnaldagi bitta yozuvga mos keladi va voqeani ro‘yxatga olish hodisadan keyin darhol amalga oshiriladi.

Operatsion tizimda hodisalarni logga yozilish uchta xavfsizlik komponentining biri hisoblanadi: autentifikatsiya, avtorizatsiya, audit - authentication, authorization, accounting.

Keylogger- kompyuter klaviaturasi bilan barcha manipulyatsiyani qo‘lga oluvchi dasturiy ta’minot yoki apparatning har qanday tarkibiy

qismidir. Koʻpincha keylogger klaviatura va OT oʻrtasida joylashgan va barcha foydalanuvchilar harakatlarini qoʻlga kiritadi.

Dastur keyloggerlari shaxsiy kompyuter foydalanuvchilari faoliyati ustidan nazoratni amalga oshiradigan dasturiy mahsulotlar guruhiga kiradi.

Apparat keyloggerlari klaviatura va kompyuter oʻrtasida biriktirilishi mumkin boʻlgan yoki klaviaturaning oʻzida joylashgan kichik qurilmalardir.

Akustik keyloggerlar - bu kompyuter klaviaturasi tugmachalari bosilganda foydalanuvchi tomonidan yaratilgan tovushlarni avval qayd etadigan qurilmalaridir, keyin qurilma bu tovushlarni tahlil qiladi va matn formatiga aylantiradi.

Trafikni qoʻlga kiritish: tarmoq interfeysini “tinglash”; kanal boʻlinishiga sniferni oʻrnatish; trafikni tarqatish (dasturiy yoki apparat orqali) va nusxani sniferga yuborish; elektromagnit nurlanishni oʻrganish; kanal (MAC- spoofing) va tarmoq (IP- spoofing) darajasida hujum uyushtirish orqali amalga oshiriladi.

Snifer tarmoq yoki boshqa uzellar uchun moʻljallangan trafikni qoʻlga kiritish va tahlillash yoki faqat tahlillash uchun moʻljallangan dasturiy yoki apparat-dasturiy vositadir.

Wireshark tarmoq uzatish analizatori boʻlib, uning vazifasi tarmoq trafigini qoʻlga kiritish va uni batafsil koʻrsatish.

Wireshark tarmoqdagi muammolarni hal qilish, tarmoq ilovalardagi nosozliklarni tuzatish, tarmoq protokollari ichki tuzilishini oʻrganish uchun ishlatiladi.

Jinoyat izlarini ikki toifaga ajratish mumkin: ichki va tashqi. Tashqi izlarga quyidagilar: aloqa kabellarida buzilgan signal qurilmalari; optik aloqa liniyalarida signallarning susayishini kuchaytirish; kuchlanish, sigʻim, qarshilik yoki chastotadagi oʻzgarishlar kiradi.

Ichki izlarga quyidagilar: telefon qoʻngʻirogʻi, qaytariluvchi kirishga muvaffaqiyatsiz urinishlar; tez-tez foydalanish soʻrovi; haqoratli yoki shafqatsiz xabarlar; oʻchirilgan yoki buzilgan ma’lumotlar; koʻchirilgan yoki oʻzgartirilgan fayllar kiradi.

Nazorat uchun savollar.

1. *Kompyuter jinoyatlarini sodir etishga olib keladigan asosiy sabab va shartlarni sanab oʻting.*
2. *Kompyuter jinoyatlarining oldini olish boʻyicha qanday tadbirlar mavjud?*
3. *Tegishlilikni va IP-manzil joyini aniqlash mexanizmi qanday?*

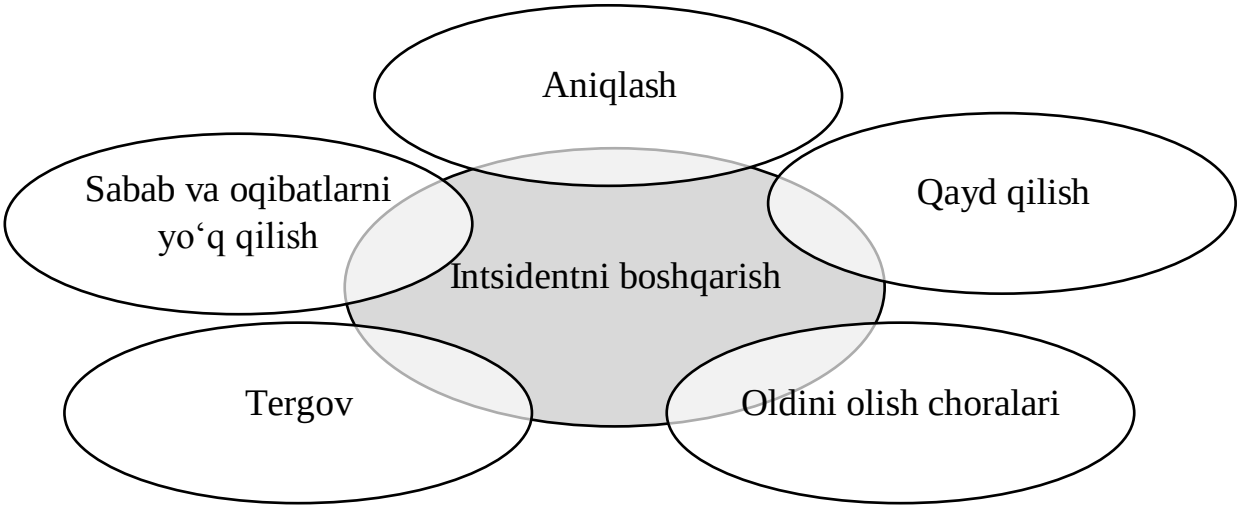
4. *Domen nomining tegishliligini aniqlash mexanizmi qanday?*
5. *Whois nima?*
6. *Loglar nimani anglatadi?*
7. *Loglarda qanday ma'lumotlar mavjud?*
8. *Veb-serverning loglarida qanday ma'lumotlarni topish mumkin?*
9. *Tajovuzkorning xatti-harakatlari haqida axborot olish, loglar orqali unga tegishli biron ma'lumotlarni olish uchun nima qilish kerak?*
10. *Windows, UNIX va Linux operatsion tizimlarining tizim loglaridagi farqlar.*
11. *Keyloggerlarning tasniflanishini shakllantiring.*
12. *Keyloggerlardan himoya usullarini keltiring.*
13. *Qanday qilib trafik qo'lga kiritiladi?*
14. *Wireshark nima uchun ishlatiladi?*
15. *Kompyuter jinoyatchilarini (xakerlarni) aniqlash uchun nima qilish kerak?*
16. *Jinoyat izlarining qanday kategoriyalari bo'lishi mumkin?*

4. RAQAMLI KRIMINALISTIKADA INSIDENTLARNI TADQIQ QILISH VA STEGANOGRAFIYA

4.1. Insidentlarni tadqiq qilish bosqichlari

Tashkilot va firmalarda insidentlarni aniqlashning usuli yo‘q, va xodimlar qanday hodisalar insidentlar bo‘lishi mumkinligi haqida ma’lumotga ega emaslar. Bu ayniqsa axborot xavfsizligi insidentlarida katta ahamiyatga ega - negaki ular har doim ham normal ish tartibini buzmaydi. Masalan, xavfsizlik insidentiga stolda maxfiy hujjatlarni qoldirishni kiritish mumkin. Buni hech kim e’tiborga olmaydi va tajovuzkor (kompaniya xodimi bo‘lishi mumkin) bunday hujjatlarni ko‘radi. Insidentlarning tadqiq qilish bosqichida quyidagilar asosiy rolni o‘ynaydi: insident qaydlari mavjud jurnallarni saqlash, foydalanuvchi vakolatini aniq ajratish, bajarilgan harakatlar uchun javobgarlik – hodisada kim ishtirok etgan va qanday harakatlar qilganini ko‘rsatadigan dalillar muhimdir. Insidentlarning oqibatlari bartaraf etilgach va biznes-jarayonlar qayta tiklangach, insidentni tekshirish, tuzatuvchi va profilaktika choralarini amalga oshirish uchun hech qanday choralar ko‘rilmaydi.

Insident - xizmatning standart operatsiyalari tarkibiga kirmagan, xizmat ko‘rsatishning to‘xtalishi yoki xizmat sifatining yomonlashishiga sabab bo‘lishi mumkin bo‘lgan har qanday hodisadir (16- rasm).



16- rasm. Axborot xavfsizligi insidenti

Insidentlarni tadqiq qilish bir qancha asosiy maqsadlar ifodalaydi:

– axborot xavfsizligi insidentlarining oqibatlarini lokalizatsiya qilish va tugatish;

– jinoyatchilarni va ularning motivatsiyalarini aniqlash, ularni javobgarlikka tortish imkoniyatlarini ta’minlash;

– insidentlar tahlili va kelgusida ham shunga o‘xshash holatlarning oldini olish choralarini ko‘rish.

Boshqa xususiy maqsadlar muayyan hodisaning aniq tergovi orqali amalga oshirilishi mumkin. Tekshiruvning yagona metodologiyasi yo‘q, lekin umuman tergov davomida quyidagi harakatlar amalga oshiriladi:

– dalillarni to‘plash va tahlil qilish;

– jinoyatchilarni aniqlash va ularni javobgarlikka tortish choralarini ko‘rish;

– insidentning sabablarini aniqlash;

– insidentlarning oldini olish bo‘yicha choralar ko‘rish uchun tavsiyalar berish;

– tadqiq materiallarini saqlash va himoya qilish.

Ba’zi muhim bosqichlarni ko‘rib chiqamiz.

Axborot xavfsizligi insidenti bo‘yicha dalillar yig‘ish - tadqiq jarayonning eng muhim qismidir, qanday maqsadda amalga oshirilishidan qat’iy nazar. Uning muvaffaqiyati asosan to‘plangan dalillarning sifatiga bog‘liq, shuning uchun dalillar qator majburiy talablarga javob berishi kerak:

– to‘liqligi (hodisani obyektiv o‘rganish uchun dalil yetarli);

– ahamiyati (dalil insidentga bog‘liq);

– aniqligi (dalillar ishonchli manbalardan olingan va o‘zgartirilmagan);

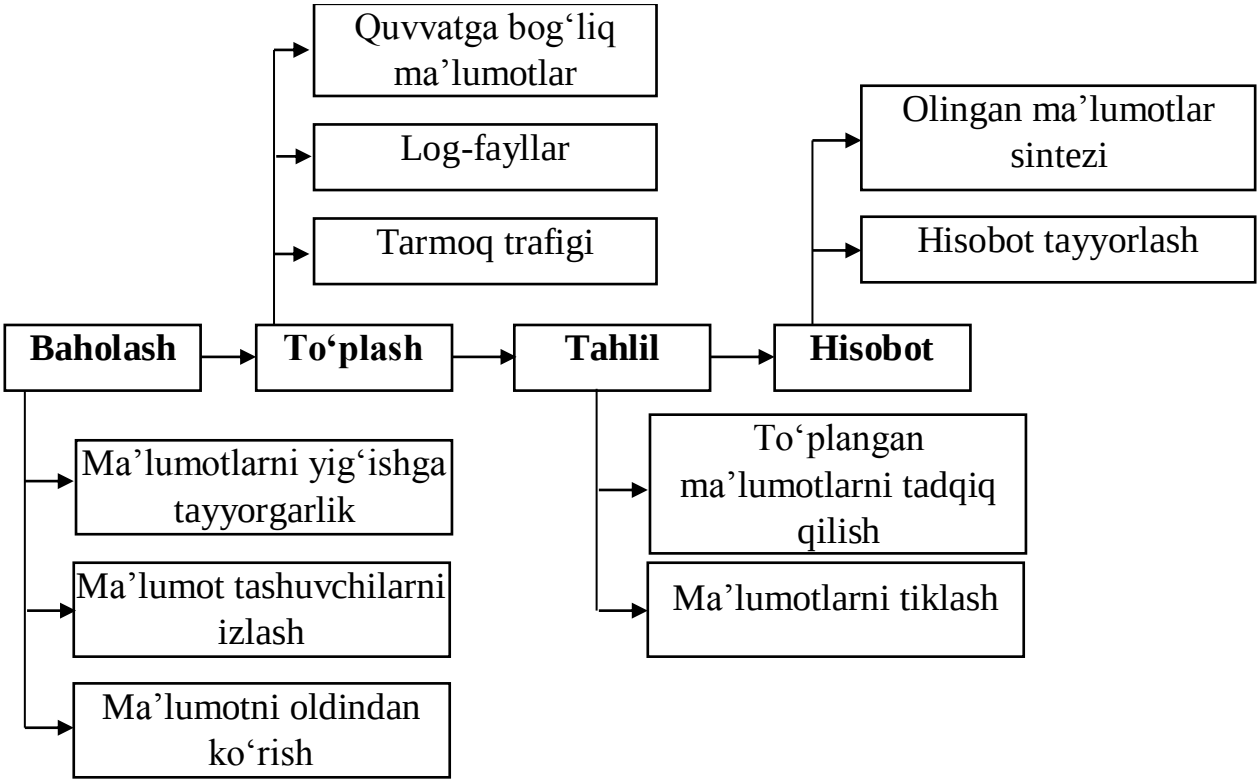
– ruxsat etilganligi (dalillar qonuniy yo‘l bilan olinishi kerak).

Tadqiqning dastlabki bosqichida, dalillarning sudda qo‘l kelishi mumkinmi yoki yo‘q, aytish qiyin (chunki, hodisaning tabiati, aybdor va uning niyatlari hali noma’lum), shuning uchun ruxsat etilganlik, aniqlik va to‘liqlik talablariga jiddiy e’tibor qaratish, “iblis mayda narsalarda yashirinadi" prinsipi bo‘yicha ish ko‘rish lozim. Bundan tashqari, jinoyat ishi bo‘yicha tergovchi yoki tezkor vakil xodimi tomonidan amalga oshirilishi mumkinligini yodda tutish kerak, agar zarur bo‘lsa, huquqni muhofaza qilish organlari bilan tezkor aloqa qilish kerak.

Insidentlarni, virus tarqalishini tadqiq qilishning asosiy maqsadi hujumning oqibatlarini, uning kelib chiqish sabablari va usullarini

aniqlashdir. Hujumning sabablari va usullarini aniqlash orqali takrorlangan hujumlar va infeksiyalarning oldini olish uchun tuzatuvchi harakatlar qilish mumkin. Axborot xavfsizligi bo‘yicha mutaxassislarning tajribasi shuni ko‘rsatadiki, hujumga uchragan yoki viruslangan tashkilot insidentning chegaralarini har doim ham to‘g‘ri aniqlay olmaydi va shuning uchun oqibatlarni baholash va bartaraf etishning iloji yo‘q. Hozirgi kunda hujum va virus tarqalish oqibatlarini bartaraf etish bo‘yicha umumiy tavsiyalar mavjud emas.

Insidentlarni tadqiq qilish xavfsizlik sohasidagi muhim vazifalardan biri hisoblanadi. Avval axborot xavfsizligi insidentlarini tadqiq jarayonini batafsil ko‘rib chiqamiz. Umuman olganda, u quyidagi ko‘rinishda bo‘ladi (17- rasm):



17- rasm. Axborot xavfsizligi insidentlarini tadqiq qilish jarayonlari

1-Bosqich. Baholash. Ushbu bosqichda axborot xavfsizligi insidenti bilan bog‘liq ma’lumotlarni to‘plash bo‘yicha tayyorgarlik ishlari olib boriladi, ya’ni tadqiq qilish imkoniyatlari ko‘rib chiqiladi (tadqiq qilish uchun ruxsat olinadi, amaldagi xavfsizlik siyosati va qonunlar tahlil qilinadi); tadqiq o‘tkazadigan guruh tarkibi belgilanadi; hodisa yuz bergan tarmoq topologiyasi o‘rganiladi;

kriminalistikaga ta’luqli ma’lumotlarning manbalari aniqlanadi va hokazo.

Bundan tashqari, baholash bosqichida hodisa bilan bog‘liq bo‘lgan kompyuterni saqlash vositasi aniqlanadi.

2-bosqich. To‘plash. Ushbu bosqichda insident bilan bog‘liq barcha ma’lumotlar yig‘iladi. Ular quyidagilardir:

– quvvatga bog‘liq bo‘lmagan axborot vositalarining tarkibi (qattiq disklar, ixcham disklar, USB flesh-disklar va h.k.);

– quvvatga bog‘liq ommaviy axborot tashuvchilar tarkibi (tezkor xotira);

– tarmoq uskunalari, serverlarning log-fayllari;

– tarmoq trafigi.

Yuqoridagi ma’lumotlarni to‘plash maxsus asboblar bilan nusxasini yaratishdan iborat.

Quvvatga bog‘liq bo‘lmagan axborot vositalarining tarkibi. Quvvatga bog‘liq bo‘lmagan vositaning nusxasini yaratmasdan oldin, dasturiy ta’minot va apparatni ro‘yxatga olish blokirovkalari ishlatiladigan kontentning yaxlitligi (o‘zgarmasligi), shuningdek, maxsus operatsion tizimlarni ta’minlash kerak. Nusxa ko‘chirish (yoki o‘chirish) kerak bo‘lgan kompyuter ishlayotgan bo‘lsa, unda quvvatga bog‘liq bo‘lmagan ma’lumotlar yig‘ilgandan so‘ng kompyuter faoliyati to‘xtaydi, quvvatga bog‘liq bo‘lmagan ma’lumot yig‘ilmasligi kerak bo‘lsa darhol to‘xtatiladi; maxsus holatlarda (masalan, o‘ta muhim serverlarni o‘chirib qo‘yish imkoni bo‘lmaganda), ishlaydigan tizimdan quvvatga bog‘liq bo‘lmagan ma’lumotlarning nusxasini ko‘chirish mumkin.

Yozuv blokirovkalari operatsion tizimning yoki uchinchi tomon dasturlarining xatosidan kelib chiqadigan xato tufayli ma’lumotni yozish xavfsiz ma’lumotlar tashuvchisini ulash imkonini beradi.

Uskuna blokatorlari ushbu ma’lumotlarni o‘qish uchun ishlatiladigan operatsion tizimlar va dasturlardan qat’iy nazar o‘z vazifalarini bajaradilar. Ixtisoslashgan operatsion tizimlar, qoida tariqasida, tadqiq qilish ostida bo‘lgan kompyuterdan ishonchli (kriminalistik) dasturiy ta’minot muhiti o‘rnatilishi orqali ma’lumot tashuvchi vositalarni nusxalash uchun ishlatiladi. Odatda, ushbu operatsion tizimlar CD yoki USB Flash vositasidan yuklanadi va yuklash jarayonida dasturiy yozuvlarni blokirovkalashni o‘z ichiga oladi. Bunday operatsion tizimlarning namunalari:

– grml;
– CAINE Live CD;
– DEFT Linux;
– e-fense Helix3 Pro.

Quyidagi dasturlar to‘g‘ridan-to‘g‘ri ma’lumotlarni ko‘chirib olish uchun ishlatilishi mumkin:

– dd (deyarli barcha Linux tarqatuvchilari tarkibiga kiradi);
– dc3dd - dd ning o‘zgartirilgan versiyasi;
– aimage;
– FTK Imager.

O‘rganishdan oldin quvvatga bog‘liq bo‘lmagan ma’lumotlarni tashuvchi vositalarning tarkibidan nusxa ko‘chirish ixtiyoriy ekanini ta’kidlash lozim - vositaning asl tarkib yaxlitligi saqlangan hollarda (masalan, vositaning sozligi yoki yozuvni bloklash qo‘llanilganda), aslning o‘rniga nusxalarini o‘rganish maqbul emas.

Quvvatga bog‘liq ma’lumotlarni to‘plash operatsion tizimlardan ularni o‘chirishdan oldin amalga oshiriladi. Odatda, quvvatga bog‘liq ma’lumotlarni yig‘ish jarayoni quyidagilardan nusxa olishdan iborat:

– kompyuterning tezkor xotira tarkibi;
– o‘rnatilgan shifrlangan fayllar va tarmoq omborlari tarkibi;
– faoliyat yurituvchi jarayonlar va xizmatlar ro‘yxati;
– joriy tarmoq ulanishlar va ochiq portlar ro‘yxati;
– o‘rganilayotgan tizimning tarmoq konfiguratsiyasi;
– muhit o‘zgaruvchilari;
– monitor ekranida foydalanuvchi ko‘rgan tasvir (ekran tasvirini yaratish).

Ushbu ma’lumotni o‘rganilayotgan operatsion tizimga nusxalash uchun tashqi ma’lumot tashish vositalari ulanishi mumkin, undan ma’lumotlarni to‘playdigan maxsus dastur ishga tushiriladi. Ba’zan tarmoq orqali tizimga maxsus dastur yuklanadi. Nusxalangan ma’lumotlar tashqi muhitda saqlanishi yoki tarmoq orqali ishonchli serverga uzatilishi mumkin.

Loglarni nusxalash bir necha usulda amalga oshirilishi mumkin:

– faqat muayyan insidentga bog‘liq ma’lumotlarga oid yozuvlarni ko‘chirib olish (masalan, muayyan bir IP-manzil yoki vaqt oralig‘iga bog‘liq);
– log fayllardan butunlay nusxa ko‘chirish;
– barcha axborot tashuvchilarini nusxalash.

U yoki bu nusxa ko‘chirish usulini tanlashda asosiy omillar quyidagilardir: loglarga bo‘lgan ishonch darajasi va shunga muvofiq, loglarining to‘g‘riligi va o‘zgarmasligi darajasini aniqlashga yo‘naltirilgan tadqiqot miqdori. Log fayllarning zararli o‘zgarishi yoki soxtalashtirilishi ehtimoli kichkina bo‘lsa, faqat log fayllarni yoki ularning alohida yozuvlarini ko‘chirib olish joizdir. Aks holda, butun tashuvchi vositasining tarkibini (tizimga ruxsatsiz kirish izlarini, log fayllarini o‘zgartirish izlari va boshqalarni qidirib topish uchun) nusxalash tavsiya etiladi.

3-bosqich. Tahlil. Ushbu bosqichda yig‘ilgan ma’lumotlarning tahlili quyidagi algoritmga muvofiq amalga oshirilishi mumkin:

– obyekt (disk, diskning nusxasi, tarmoq trafigi dampi va boshqalar) haqida umumiy ma’lumot olish;

– ma’lumotlarni ochiq holatda o‘rganish;

– bilvosita (masofadan, yashirin, shifrlangan) shaklda ma’lumotlarni o‘rganish.

Quvvatga bog‘liq bo‘lmagan ma’lumot tashuvchi vositalarni va ularning nusxalarini o‘rganish ko‘p hollarda fayl tizimlarining tarkibini o‘rganish va ma’lumotlarni tiklashdan iborat. Fayl tizimlarini tadqiq qilish tajovuzkorning harakatlaridan kelib chiqadigan turli xil axborot izlarini tahlil qilish, tergov qilinayotgan tizimning dasturiy ta’minotini va uskunasini tahlil qilishdan iborat. Fayl tizimlarida ushbu izlarning soni (kriminalistik ahamiyatga ega ma’lumotlar manbai sifatida) juda katta bo‘lib, shuning uchun insidentlarni tekshirishda fayllar tizimini kriminalistik tadqiq qilish uchun keng qamrovli usullar va algoritmlar mavjud emas.

Fayl tizimlarini kriminalistik tadqiq qilish uchun quyidagi dasturiy mahsulotlardan foydalanish mumkin:

– EnCase Forensic;

– Forensic Toolkit;

– The Sleuth Kit.

Quyidagi dasturlar ma’lumotlar uzatish uchun ishlatilishi mumkin:

– Foremost;

– PhotoRec.

Tarmoqli paketlar dampining tahlillari quyidagicha:

– tarmoq paketlari va ulanishlarining xususiyatlarini aniqlash (masalan, maxfiy ma’lumotlarni qidirish uchun);

– tarmoq orqali uzatiladigan xabarlarni chiqarish (masalan, axborot tarqalish kanallarini qidirish uchun).

Birinchi holda tarmoq paketlarini analizatorlari quyidagilar qo‘llanilishi mumkin:

– Wireshark;

– Network Miner.

Ikkinchi holatda odatda tarmoq paketlarini tahlil qiladigan mutaxassislar emas, balki turli xil tarmoq xabarlarini (elektron pochta xabarlari, internet peygerlar, va hokazo) izlash, chiqarish va saqlash jarayonlarini avtomatlashtirishga imkon beruvchi yuridik qo‘lga olish tizimlari, shuningdek, kalit so‘zlar va qo‘lga olinuvchi ma’lumotlarning boshqa mezonlarini kiritishdan foydalaniladi.

4-bosqich. Hisobot. Ushbu bosqichda tahlil qilish bosqichida olingan barcha ma’lumotlarning sintezi, so‘ngra hisobotni u mo‘ljallangan auditoriya uchun tushunarli bo‘lgan shaklda yozish amalga oshiriladi. Hisobot quyidagilarni o‘z ichiga olishi mumkin:

– insident sabablari haqida ma’lumotlar;

– insidentga aloqador shaxslar to‘g‘risidagi ma’lumotlar;

– insident xronologiyasi;

– tahlil davomida aniqlangan izlar (dalil) ning batafsil tavsifi;

– jarayon davomida qo‘llanilgan tadqiq qilish usullari, dasturiy va apparat ta’minot, ularni qo‘llash holatlari haqida ma’lumot;

– kelajakda shunga o‘xshash insidentlarni oldini olish uchun tavsiyalar.

Insident haqida xabardor etish. Avvalo insident haqida ma’lumot olish kerak. Bu haqida xavfsizlik siyosatini shakllantirish va xodimlar uchun axborot xavfsizligida ta’lim bo‘yicha prezentatsiyalar yaratish bosqichida o‘ylash zarur.

Axborotning asosiy manbalari:

1. *Helpdesk.* Odatda qurilmadagi har qanday nosozlik AT-servisning yordam paneliga yoziladi yoki telefon orqali xabar beriladi. Shuning uchun, "xelpdesk" ish jarayoniga oldindan "integratsiya qilinish" va talabnomaning axborot xavfsizligi bo‘limiga o‘tkazilishi kerak bo‘lgan insidentlar turlarini ko‘rsatish kerak.

2. *Foydalanuvchilardan bevosita xabarlar*. Bitta aloqa nuqtasini tashkil qiling va bu haqda xavfsizlik xodimlari uchun treningda xabar bering. Hozirgi kunda tashkilotlarda axborot xavfsizligi bo‘linmalari

odatda juda katta emas, ko‘pincha 1-2 kishidan iborat. Shuning uchun u insidentlar uchun javobgarni tayinlash qiyin bo‘lmaydi, IS Helpdesk ehtiyojlariga ko‘ra elektron pochta manzillarini aniqlashtirish bilan ovora bo‘lishning keragi yo‘q.

3. ***Xavfsizlik xodimlari tomonidan topilgan insidentlar*****.** Bunda har bir narsa oddiy va bunday qabul qilish kanalini tashkil qilish uchun hech qanday imo-ishora talab qilinmaydi.

4. ***Loglar va ogohlantirish tizimlari*****.** Antivirus, IDS, DLP va boshqa xavfsizlik tizimlarining konsolida ogohlantirishlarni sozlang. Tashkilotda o‘rnatilgan dastur va tizimlar loglaridan ma’lumotlarni to‘playdigan agregatorlardan foydalanish ancha qulaydir. Tashqi tarmoq bilan aloqador nuqtalarga va sezgir axborotni saqlash joylariga alohida e’tibor berilishi kerak.

4.2. Insidentlarni boshqarish

Insidentni boshqarish - axborot xavfsizligini boshqarish kabi raqamli kriminalistikada ham eng muhim tartiblardan biri. Avvalo, insidentning oqibatlarini to‘g‘ri va tezda bartaraf etish, shuningdek, buning uchun qanday choralar ko‘rish kerakligini nazorat qilish muhimdir. Bundan tashqari, insidentning sabablarini bartaraf etish bo‘yicha harakatlar zarurligini baholash kerak, agar kerak bo‘lsa - ularni amalga oshirish, shuningdek, hodisaning takrorlanishiga yo‘l qo‘ymaslik uchun choralarni ko‘rish talab qilinadi. Keyingi navbatda, axborot xavfsizligi insidentlari haqidagi barcha ma’lumotlarni saqlash juda muhim, chunki axborot xavfsizligi insidentlari statistikasi ularning soni va tabiatini, shuningdek, vaqt o‘tishi bilan bog‘liq o‘zgarishlarni tushunishga yordam beradi. Insidentlar statistikasi to‘g‘risidagi ma’lumotlardan foydalanish yordamida kompaniya uchun eng dolzarb tahdidlarni aniqlash mumkin, natijada kompaniyaning axborot tizimining xavfsizlik darajasini yaxshilash uchun mumkin bo‘lgan reja ishlarini aniq belgilash mumkin. Bularning barchasi axborot xavfsizligi insidentlarini boshqarish bo‘yicha alohida hujjatlashtirilgan va tasdiqlangan protsedurasini yaratish uchun keltiriladi, ammo ular ushbu jarayonning ahamiyatini tushunish uchun yetarlidir.Ko‘pgina kompaniyalarda axborot xavfsizligi insidentlarining soni va tabiatdagi o‘zgarishlarni kuzatib borish har doim ham mumkin emas, sababi, insidentlarni boshqarish tartibi mavjud emas. Ko‘pincha, insidentlarning yo‘qligi xavfsizlikni boshqarish tizimining to‘g‘ri ishlayotganligini

bildirmaydi, balki insidentlar aniqlanmagan degan ma’noni anglatadi. Odatda, insidentlarni boshqarishdagi asosiy qiyinchiliklar quyidagilardir.

Insident sodir bo‘lganligi haqida ogohlantirish. Ko‘pincha tashkilot xodimlari insident sodir bo‘lgan taqdirda kimni va qay tarzda xabardor qilinishi kerakligi haqida ma’lumotga ega emaslar, - masalan, hisobotlarni shaklini yoki insident haqidagi hisobotlarni yuborish kerak shaxslarning ro‘yxatini belgilangan emas. Hatto agar xodim boshqa hamkasbi o‘z uyiga maxfiy hujjatlarni olib ketayotganini payqasa ham, bu holatda qanday choralar ko‘rish kerakligini har doim ham bilmaydi.

Insidentni qayd etish. Mas’ul shaxslar odatda insident yozish usullari bilan ta’minlanmaydilar. Ro‘yxatga olishning maxsus qoidalari, shuningdek, qoidalar va muddatlar mavjud emas. Insidentlar misollari sifatida kompaniya veb-saytidagi ma’lumotlarning ruxsatsiz o‘zgartirilishi, kompyuterni blokdan chiqarib yuborilganligi, korporativ yoki shaxsiy pochta orqali maxfiy ma’lumotlarni yuborish kabi hodisalarni keltirish mumkin. Insident, birinchi navbatda, hal qilinmagan hodisa bo‘lganligi sababli, kimdir tomonidan taqiqlanishi kerak, shuning uchun tizimda bajarilishi mumkin bo‘lgan va taqiqlangan barcha harakatlar aniq tasvirlangan hujjatlar bo‘lishi zarur. Misol uchun, kompaniyalardan birida xodim shifrlash vositalarini ishlatmasdan, kompyuterda maxfiy ma’lumotni saqlab qoladi. Ishdan so‘ng u kompyuterni uyiga olib kirib, uyning derazalari ostida qoldirgan mashinada unutdi va kechasi mashina qulfi buzilib, kompyuterni o‘g‘irlab ketishdi. Hujumchilar kompaniya maxfiy ma’lumotlariga ega bo‘lishdi va uni raqiblarga sotishdi. Bundan tashqari, boshqa axborot vositalarida saqlanmagan qimmatbaho ma’lumotlar kompyuterda saqlangan. Bunday insident kompaniyaning kompyuterlardagi ma’lumotlarni saqlash bo‘yicha protseduralarni ishlab chiqmaganligi sababli sodir bo‘lishi mumkin edi. Kompyuterni ofisdan tashqariga ko‘chirish, shifrlash va zaxira ma’lumotlarining yo‘qligi kompaniyaning kompyuterlarda axborotni saqlash sodir bo‘lishi mumkin bo‘lgan xatolar va tabiiyki insident sababchilaridir.

Biroq bu hujjatlashtirilmaguncha (ya’ni buning taqiqlanganligi hujjatlarda tavsiflanmaguncha), xodimning javobgarlikka tortish va takroriy sodir etilishiga yo‘l qo‘ymaslik mumkin emas. Hodisalarni kuzatish, foydalanilmayotgan akkauntlarni vaqtida o‘chirish, foydalanuvchi xatti-harakatlarini monitoring va nazorat qilish, tizim ma’murlari faoliyatini nazorat qilish va hokazo muhim ahamiyatga ega.

Kompaniyalardan birida quyidagi hodisa qayd etildi: ishdan boʻshatilganda tizim maʼmuri kompaniya tomonidan ishlab chiqilgan dasturiy taʼminot mahsulotini oʻgʻirlab, dasturni oʻz savdo belgisi ostida bozorga chiqarib raqiblarga topshirdi. Bundan tashqari, u axborot tizimiga oʻzgartirishlar kiritdi, natijada, uning ketishi natijasida baʼzi qismlarining ishlashi toʻxtatildi. Bu ishda maʼmurni javobgarlikka tortish mumkin emas edi, chunki, birinchi navbatda, uning harakatlarini roʻyxatga olish amalga oshirilmadi, ikkinchidan, maʼmur oʻzining noqonuniy harakatlarining barcha dalillarini olib tashlashi mumkin, uchinchidan, insident sodir boʻlganligi toʻgʻrisida dalillarni toʻplash tartibi oʻrnatilmagan. Bundan tashqari, kompaniyada bunday holatlarda nima qilishni kerakligini bilishmas edi.

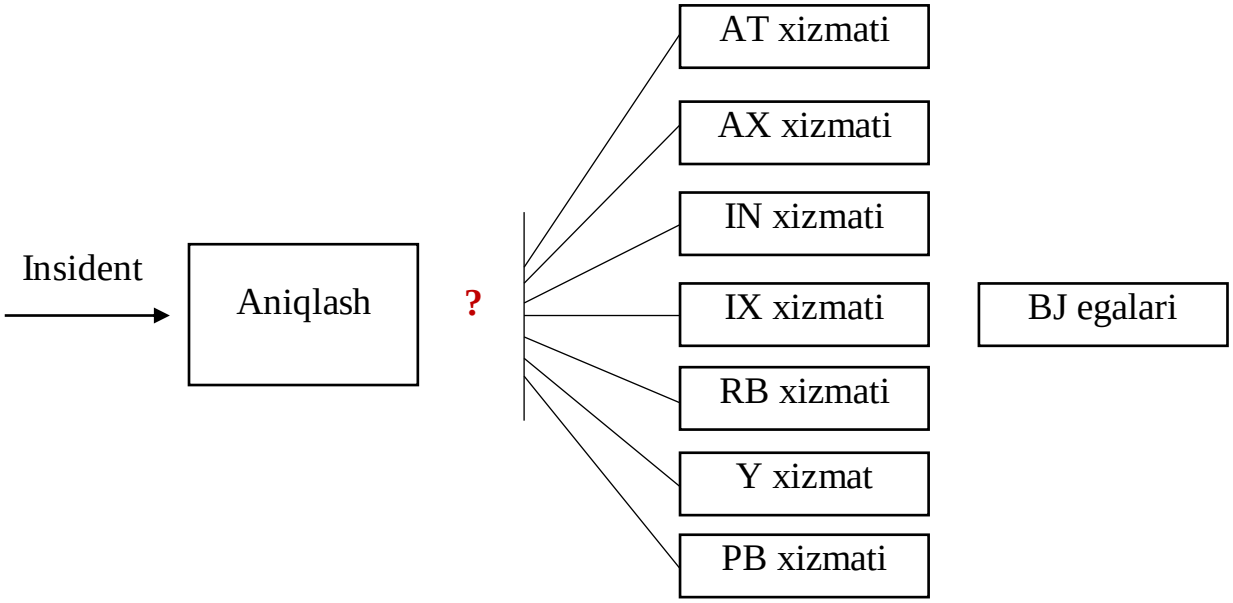
Insidentni aniqlash va roʻyxatga olish. Axborot xavfsizligi insidenti foydalanuvchi yoki tizim maʼmuri tomonidan sezilishi mumkin. Odatda, maʼmurlar foydalanuvchilardan farqli oʻlaroq hodisalar aniqlanganda nima qilish kerakligini biladi. Foydalanuvchilar uchun qoida tariqasida ish beruvchi insident sodir boʻlganda murojaat etish shakli, masʼul shaxslarning koordinatlarini, shuningdek, xodim oʻz-oʻzidan amalga oshirishi mumkin boʻlgan harakatlar roʻyxatini (yoki qaysi xatti-harakatning mustaqil bajarilishi taqiqlanganligi haqida ogohlantirish) taqdim etishi kerak. Bunday hisobotda hodisaning batafsil tavsifi, hodisaga bogʻliq xodimlar roʻyxati, hodisani qayd etgan xodimning ismi, hodisaning kelib chiqishi va roʻyxatga olinishi sanasi koʻrsatilishi kerak. Shunday qilib, har bir xodim masalan, agar u hujjat bilan ishlashni davom ettirsa va oxirgi paytlarda oʻz hujjatiga haqiqatga mos kelmagan oʻzgarishlar kiritilganini va muallif nomaʼlumligini sezgan holda uning harakatlari qanday boʻlishi kerakligini aniqlaydigan koʻrsatma oladi.

Keyinchalik, insidentni roʻyxatga olishni oʻz zimmasiga olgan mutaxassis uchun koʻrsatmalar ishlab chiqish kerak. Insidentni aniqlagan xodim insident qayd etish va keyingi harakatlarni bajarish uchun masʼul boʻlgan xodimga murojaat qiladi. Kichkina kompaniyalarda xodimlar bevosita aloqa qiladilar, ular hodisaning oqibatlarini va sabablarini bartaraf eta oladilar. Juda katta kompaniyalarda, odatda, hodisani qayd etadigan va insident haqidagi maʼlumotni tegishli mutaxassislarga joʻnatadigan xodim tayinlanadi. Bunday yoʻriqnomada, masalan, hodisani roʻyxatga olishning qoidalari va muddati, hodisani aniqlagan xodim uchun zarur boʻlgan dastlabki koʻrsatmalar roʻyxati, shuningdek, insident haqidagi

ma’lumotni tegishli mutaxassisga yetkazish tartibi, oqibatlarini bartaraf etishni monitoring qilish tartibi va hodisaning sabablari ko‘rsatiladi.

Insidentni aniqlash doimo og‘ir. Xodimlar hodisa bartaraf qilishga yetaklovchi barcha zarur harakatlardan bosqichma-bosqich xabardor bo‘lishi kerak (18- rasm).

Bunday vaziyatda aniq yo‘riqnomalar mavjud bo‘lmasa va o‘qitishning tegishli darajalari bo‘lmasa, insidentlarga javob jarayoni hodisalarni aniqlash va bartaraf etishning stoxastik harakatiga aylanadi. Odatda, bir kishi bajarishi kerak bo‘lgan vazifalar bir nechta xodimlar orasida "tarqalgan" bo‘lib, natijada ular parallel ravishda harakat qiladi va faqat qimmatli vaqtni yo‘qotadi.



18- rasm. Axborot xavfsizligi insidentlarini aniqlash

AT – axborot texnologiyalari.
AX – axborot xavfsizligi.
IN – ichki nazorat.
IX – iqtisodiy xavfsizlik.
RB – risklarni boshqarish.
Y – yuridik.
PB – personalni boshqarish.
BJ – biznes-jarayonlari

Insidentning sabablari va oqibatlarini bartaraf etish va uni tadqiq qilish. Insidentning sabablari va oqibatlarini bartaraf etish bo‘yicha kiritilishi kerak bo‘lgan ko‘rsatmalarga umumiy harakatlarning tavsifi (har bir hodisa turi uchun muayyan harakatlar murakkab va har

doim belgilanishi mumkin emas), shuningdek, hodisaning oqibatlari va sabablarini bartaraf etish muddati kiradi. Vaziyatni bartaraf etish shartlari va hodisaning sabablari insidentning darajasiga bog‘liq. Insidentlar tasnifini ishlab chiqish kerak - insidentlarning kritik darajasini aniqlash, har bir darajadagi insidentlarni va ularni bartaraf etish muddatini ta’riflash lozim. Kompaniyadagi hodisalarni insident deb hisoblash kerakligini belgilaydigan hujjat shuningdek, insidentlar darajasini tasvirlab berish kerak.

Shunday qilib, insidentning oqibatlari va sabablari bilan qanday kurashish bo‘yicha ko‘rsatmalar quyidagilarni o‘z ichiga olishi mumkin: insidentning oqibatlari va sabablarini bartaraf etish, qaror qabul qilish muddati va ko‘rsatmalarga rioya qilmaslik uchun javobgarlikka tortish harakatlarining tavsifi.

Insidentni tadqiq qilish uning yuzaga kelishi uchun mas’ul shaxslarni aniqlash, hodisaning dalillarini to‘plash, tegishli intizomiy harakatlarni o‘z ichiga oladi. Katta insidentlarni tekshirish bo‘yicha komissiya tuziladi (uning tarkibiga sodir bo‘lishi mumkin bo‘lgan insidentni yozuvchi xodim kiradi). Insidentlarni tadqiq qilish bo‘yicha ko‘rsatma quyidagilarni tasvirlashi kerak: hodisani tekshirish bo‘yicha harakatlar (shu jumladan, uning yuzaga kelishi uchun mas’ul shaxslarni aniqlash), dalillarni yig‘ish va saqlash qoidalari (ayniqsa, sud tizimida dalillarni qo‘llash zarur bo‘lishi mumkin) va intizomiy harakatlar qoidalari.

4.3. Insidentni toifalash va klassifikatsiyasi

Garchi xavfsizlik insidentlari xilma-xil bo‘lsa-da, ular statistikani saqlash osonroq bo‘lgan bir necha toifaga bo‘linadi.

1. Maxfiy yoki ichki axborotni oshkor qilish yoki bunday oshkor qilishga tahdid. Buning uchun, eng kamida, maxfiy axborotning hozirgi ro‘yxatini, elektron va qog‘oz axborot vositalarini belgilashning faoliyat yurituvchi tizimiga ega bo‘lish kerak. Yaxshi misol - korxona ichki portalida yoki ichki fayllarni saqlash muhitida joylashgan deyarli barcha hayotiy vaziyatlar uchun yaratilgan hujjat andozalari odatiy ravishda "Faqat ichki foydalanish uchun" deb belgilanadi.

2. Ruxsatsiz kirish. Buning uchun himoyalangan resurslar ro‘yxatini kiritish kerak. Boshqacha aytganda, tashkilotning, mijozlarning yoki pudratchilarning ma’lumotlari qayerda saqlanishini bilish lozim. Bundan tashqari, bu toifaga nafaqat kompyuter tarmog‘iga ruxsatsiz kirish, balki binolarga ruxsatsiz kirishni ham qo‘shish maqbul.

3. Vakolatning ortishi. Bu punktni oldingisi bilan birlashtirilish mumkin, lekin ularning ajratilishi maqsadga muvvofiqdir. Ruxsatsiz kirish deganda tashkilotning resurslari yoki binolariga kirish huquqiga ega bo‘lmagan shaxslarning kirishi tushuniladi. Bu tizimga kirish uchun huquqqa ega bo‘lmagan tashqi tajovuzkordir. Vakolatning ortishi - tashkilot xodimlarining har qanday manbalariga va binolariga ruxsatsiz kirish huquqidir.

4. Virusli hujum. Bunday holda, quyidagilarni tushunish kerak: xodimning kompyuterida bitta virusli hujum atroflicha ko‘rib chiqishga olib kelmasligi kerak, chunki bu inson omiliga bog‘liq bo‘lishi mumkin. Agar tashkilotning kompyuterlari sezilarli darajada zararlangan bo‘lsa, unda to‘liq inshootni xavfsizlik bilan bog‘liq zararlanish manbalari, sabablari va h.k.lar uchun kerakli izlanishlar bilan ta’minlanishi kerak.

5. Qaydlar ro‘yxatining kompрometatsiyasi. Ushbu punkt 3-punkt bilan umumiy fikrga ega. Agar foydalanuvchi insident vaqtida jismonan va aqlan o‘zining qayd ro‘yxatlarini qo‘llay olmasa, insident 3-punktdan 5-punktga o‘tadi.

Axborot xavfsizligi insidentlarini tasniflashning asosiy maqsadi insidentga javob reaksiyasi jarayonini ko‘rsatishda tizimlilik darajasini oshirish va subyektivlikni kamaytirishdan iborat. Ushbu jarayonlar insidentga keyinchalik javob reaksiyasini bildirish uchun insident atributlarini aniqlash va qayd etish yo‘li bilan hamda axborot xavfsizligi insidentlari menedjmentining tizimini tahlil qilish orqali amalga oshiriladi.

Axborot xavfsizligi insidentlarini quyidagi funksiyalar bo‘yicha tasniflash tavsiya etiladi:

– insidentning qayta yuzaga kelishi ehtimoli bo‘yicha;

– insidentlarga sabab bo‘lgan tahdid manbalari turlari bo‘yicha;

– insidentning sabablari bo‘yicha (tasodifiy, qasddan, noto‘g‘ri);

– insidentni amalga oshirishda jalb qilingan (ta’sir ostiga tushgan) axborot infratuzilma obyektlari turlari bo‘yicha;

– insident sodir bo‘lgan axborot infratuzilmasi darajasiga ko‘ra;

– axborot xavfsizligining buzilgan xususiyatlariga (maxfiylik, yaxlitlik, mavjudligi) ko‘ra;

– insidentning turi bo‘yicha (sodir bo‘lgan insident, amalga oshirish uchun urinish, hodisa sodir bo‘lishiga shubha-gumon);

– insidentning doirasi va harakati bo‘yicha;

– insidentni aniqlash murakkabligi bo‘yicha;
– insidentni yopishning murakkabligi bo‘yicha.

4.4. Insidentni tadqiq qilish elementlari

Insidentni tadqiq qilish uning yuzaga kelishi uchun mas’ul shaxslarni aniqlash, hodisaning dalillari va izlarini to‘plash, tegishli intizomiy harakatlarini ta’riflashni o‘z ichiga oladi. Katta shirkatlarda, odatda, axborot xavfsizligi insidentlarini tekshirish bo‘yicha komissiya ajratadi (uning tarkibiga insidentlarga javob beruvchi xodim ham mavjud).

Insidentlarni tergov qilish bo‘yicha ko‘rsatma quyidagilarni tasvirlashi kerak: hodisani tekshirish bo‘yicha harakatlar (shu jumladan, uning yuzaga kelishi uchun mas’ul shaxslarni aniqlash), dalillarni yig‘ish va saqlash qoidalari (ayniqsa, sud tizimida dalillarni qo‘llash zarur bo‘lishi mumkin) va intizomiy harakatlar qoidalari.

Kompyuter insidentlarini tadqiq qilishning 5 ta elementini ko‘rib chiqamiz.

1- element. Nima buzildi?

Quyidagilarni aniqlash juda muhim:

– *insident natijasida qanday tizim jarohatlangan;*
– *qaysi servis buzildi;*
– *qaysi ma’lumotlarga tajovuz qilingan.*

Bu maqsadda, tezkor javob berish uchun oldindan tayyorlangan operativ javob berish uchun utilitlar paketidan foydalanish mumkin. Bu insident natijasida nima buzilganligini aniqlashga yordam beradi. Ushbu paketga qaysi vositalar kiritiladi va ulardan qanday foydalaniladi.

Birinchidan, qisqa vaqt ichida *yo‘q bo‘lib ketishi* mumkin bo‘lgan ma’lumotlarni aniqlash va to‘plash zarur, bu vaqtinchalik fayllar, cookies -fayllar bo‘lishi mumkin, lekin faqat ular emas.

Ikkinchidan, normal holatdan chetga chiqishlarning mavjudligini aniqlash uchun *tarmoq ulanishlarini* va tizim faoliyatini tahlil qilishni o‘rganish kerak.

Uchinchidan, *jarayonlarni* tahlil qilishni o‘rganish kerak, kod jarayonlarda amalga oshiriladi, jarayonlar olib boriladigan fayllar va kutubxonalarda joylashgan kodni bajarishi sababli bu yerda ushbu fayllarning yaxlitligiga e’tibor beriladi.

To‘rtinchidan, jarayonlar parametr do‘konidan, *reyestrdan foydalanadi*, uning tahlillari qo‘shimcha ma’lumotni ochib beradi, bunda turli ro‘yxatga olish brauzerlari yordam beradi.

Beshinchidan, barcha jarayonlar *xotirada amalga oshiriladi*, shuning uchun xotira tahlili ham tergov uchun muhimdir.

Muammo shundaki, xotira katta, zararli ma’lumotlar esa kichik va osongina o‘n oltinchi dampda yo‘qolib qoladi.

Audit tizimi va tarmoq trafigini *monitoring qilish tizimi* ma’lumotlarning yaxlitligini buzishganini sezishga qodir.

2-element. Nima vositasida buzildi?

Quyidagilarni aniqlash juda muhim:

– *konfiguratsiyada xato mavjudmi;*
– *ilovada xato mavjudmi;*
– *tizimda xato yuz berganmi;*
– *protokolda xato yuz berganmi.*

Har bir mavzu uchun jarayonlar, reyestr kalitlari, fayllar, turli damplar va jurnallar haqida ma’lumot qanday yordam berishi mumkinligini batafsil o‘rganish uchun modul ajratamiz.

Bu yerda bir muhim narsani o‘rganish kerak: insidentlar, jurnal yozuvlari va tizim konfiguratsiyasining bir-biriga mutanosibligi. Buning uchun, har bir servisning o‘z jurnallariga bo‘lishi, u mahalliy sifatida ham, masofaviy serverda ham saqlanishi hamda turli platformalar turli xil jurnal formatlarini ishlatishi mumkinligini tushunib olish kerak.

3-element. Kim buzgan?

Quyidagilarni aniqlash juda muhim:

– *buzib kirish qaysi tizim orqali sodir bo‘lgan;*
– *hujumning yakuniy maqsadi nima edi;*
– *qaysi kompyuterdan hujum boshlangan.*

Turli jurnallardan axborotni xavfsizlik insidentidan oldingi hodisalar bilan bog‘lash qobiliyati bu yerda ham asqotadi. Ammo, bu bosqichda avvalgi bosqichlarda to‘plangan ma’lumotlardan kelib chiqib tajovuzkor identifikatorlarini aniqlab olish kerak. U IP bo‘lishi shart emas, u elektron pochta manzili, ilovadagi hisob, media fayl bo‘lishi mumkin.

4-element. Gumondor kompyuterida.

Quyidagilarni aniqlash juda muhim:

– *qanday dastur ishlatilgan;*

– *qanday fayllar ishlatilgan;*
– *hujum qaysi ketma-ketlikda sodir bo‘lgan.*

Harakat, gumondorning kompyuteri yoqilgan yoki yoqilmaganligiga bog‘liq. Agar o‘chirilgan bo‘lsa, metodologiyaga ko‘ra endi yoqilmaydi, lekin diskning nusxasi olinadi va keyinchalik AccessData FTK va EnCase kabi vositalarni ishlatib, dalillar topib, hisobot tuziladi. Dalillar kompyuterdan emas, balki printer, kseronusxa apparati, mobil qurilma kabi boshqa vositalardan topilishi mumkin.

5-element. Oldingi elementlarni asoslash.

Quyidagilarni aniqlash juda muhim:

– *nima dalil bo‘lishi mumkin?*
– *dalillarni qanday to‘plash mumkin;*
– *dalillarni qanday tahlil qilish kerak;*
– *qanday qilib tadqiq qilish hisobotini tayyorlash kerak.*

Damplar, loglar, fayllar - kompyuter terminlari. Ularni rasmiylashtirilgan tadqiq jarayoniga qo‘shilish uchun ular dalillar sifatida hujjatlashtirilishi va dalillarning huquqiy ahamiyatini saqlab turadigan tartiblarga muvofiq qayta ishlanishi kerak.

Tadqiqning mohiyati quyidagilardan iborat: tashkilot mutaxassislari hodisani aniqlaydilar yoki o‘z-o‘zidan insidentga zudlik bilan javob qaytaradilar, ma’lumotlarni tahlil qilib, tahlil natijalarini ma’muriyatga topshirishadi yoki ish yuritishni huquqni muhofaza qilish organlariga topshirilgunga qadar tadqiq qilishni texnik va huquqiy jihatdan qo‘llab-quvvatlashni ta’minlaydigan kompyuter insidentlarini tekshirish uchun tashqi ishchilarni yollashadi.

Tashkilot hodisalarni o‘rganish metodologiyasini qo‘llash uchun hodisalarni qonuniy jihatdan tegishli tekshiruvlar o‘tkazish niyatida bo‘lmasa ham, korporativ axborot tizimining umumiy xavfsizligini oshiradi.

4.5. Insidentni pretsedentli tahlili

Pretsedentli tahlil. Dastlabki tahlil tizimlarida yechimlarni izlash analogiya tushunchasiga (muayyan toifadan muayyan toifaga qarab qidirish) asoslangan. Pretsedentli tahlil va joriy vaziyat o‘xshashliklarni topish zarur bo‘lgan narsalar kabi ko‘rinadi va bu holat uchun adolatli bo‘lgan faktlarni uzatish orqali ushbu insidentga doir bir nechta xulosa chiqarish mumkin. Odatdagidek, pretsedent quyidagilardan iborat:

- muammoli vaziyatning tavsifi;
- ushbu muammoni bartaraf etish uchun muammoni hal qilish harakatlari (muammoni hal etuvchi yechim);
- va ba'zi hollarda - qarorni qo'llash natijasi.

Ko'p o'lchovli vektorning parametrik ifodasini eng aniq pretsedent tarkibi sifatida ifodalash mumkin:

$$CASE = (x_1, x_2, \dots x_p, R),$$

bu yerda, $x_1, x_2, \dots x_p -$ pretsedent tasvirlagan o'xshash ma'lumotlar parametrlari;

$R -$ bu muammoni hal qilish uchun bir yoki bir nechta yechimlar (tashxis, tavsiyalar).

Vaziyatlarga asoslangan xulosa to'rt asosiy bosqichni o'z ichiga oladi va CBR-sikl (pretsedentlarga asoslangan fikrlash davri) tashkil etadi, bularga quyidagilar kiradi:

– vaziyatlar bazasidan hozirgi holat uchun mos vaziyatlarni ajratib olish;

– mavjud muammoni hal qilish uchun pretsedentni qayta ishlatish;

– ushbu muammoni hal qilishda yechimni qayta ko'rib chiqish va moslashtirish;

– yangi qarorni yangi pretsedentning bir qismi sifatida saqlab qo'yish.

Muayyan obyektning o'ziga xos xususiyatlarini va hal qilinishi kerak bo'lgan vazifalar doirasini hisobga olgan holda, soddalashtirilgan CBR- siklidan foydalanish mumkin. Shunday qilib, pretsedent apparati vositalarini ishlatishdan asosiy maqsad operatorga yechimni taqdim etishdir. Hodisalarni ajratib olish mutanosiblik (metrik) F funksiyasini aniqlashga asoslanadi, uning qiymati esa bu pretsedent va hodisaning o'xshashligini belgilaydi. Xususiyat makonida maqsadga mos keladigan nuqta aniqlanadi va ishlatiladigan metrika doirasida eng yaqin pretsedent tanlanadi.

Rasman hodisaning analogiyasi

$x_1, x_2, \dots x_p -$ va hozirgi holati;

$k = (x_{k1}, x_{k2}, \dots x_{kp})$ ko'rish funksiyasi bilan tasvirlanadi.

$$SIM(g,k) = F(sim(x_{g1}, x_{k1}), \dots, sim(x_{gp}, x_{kp})),$$

bu yerda $sim(x_{gi}, x_{ki})$ g-hodisadagi i-xususiyatining hamda joriy k vaziyatdagi (insident) $i -$xususiyatning mahalliy o'xshashlik qiymati. F

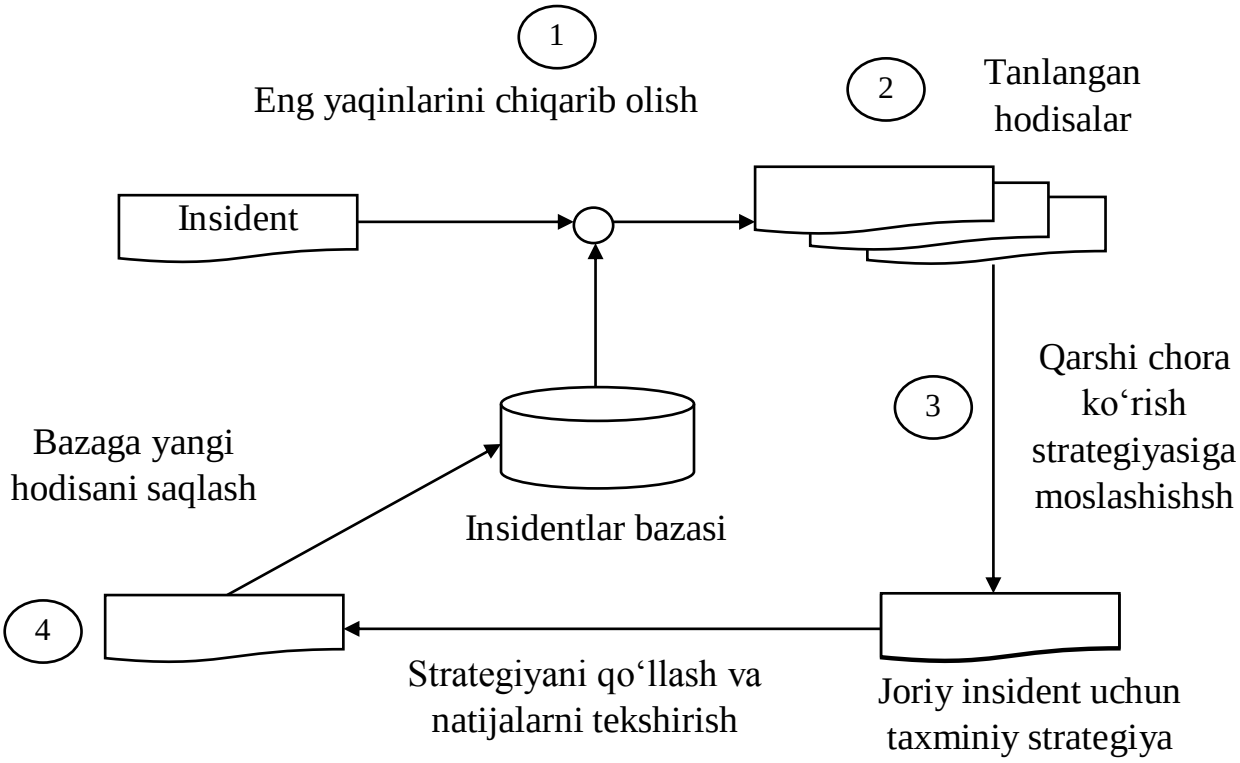
funksiya hozirgi vaziyat va hodisaning to‘liq o‘xshashliligini bildiradi. Ma’lumot bazasida shunga o‘xshash holatlar bo‘lmasa, bu yondashuv vaziyat uchun zaruriy yechimga olib kelmaydi. Agar CBR-sikli bazani fikrlash jarayonida to‘g‘ridan-to‘g‘ri to‘ldirish imkoniyatini ta’minlasa, ushbu muammoni hal qilish mumkin. Axborot xavfsizligi insidentlarini boshqarishda birinchi qadam - bu insidentlarni bevosita qayd etishdir. Keyingi xatti-harakatlar sinfga asoslanib har bir insident uchun javob choralarini qo‘llashni o‘z ichiga oladi. Ushbu bosqichda quyidagi muammolarni aniqlash mumkin:

- insident har doim to‘g‘ri tasniflanmaydi;
- har bir insidentning ma’lum darajada individual ekanligi sababli ma’lum bir sinfga taalluqli insidentga qarshi yagona javob berish strategiyasi yo‘q;
- ilgari sodir bo‘lmagan insidentlar mavjud va shuning uchun bunday hodisalar uchun tegishli javob choralari mavjud emas.

Insidentni boshqarish jarayonini yaxshilash uchun hodisa tahlildan foydalanish tushunchasi quyidagichadir. Ko‘plab G ma’lum insidentlar, ko‘plab R aniq javob strategiyalari mavjud. $G \to R$ ko‘rinishi- bu hodisadir, negaki u insidentning tavsifi va unga mos javob berish strategiyasi mavjud juftlikdir. Yangi insident qayd etilganda, unga o‘xshash hodisa topilib, undan so‘ng ushbu insident uchun pretsedentning yechimlari qo‘llaniladi. Ushbu yondashuvni amalga oshiruvchi tizimning mantiqiy tuzilishi 19-rasmda keltirilgan. Avval ma’lum bo‘lmagan va aniq javob qaytarish strategiyasiga ega bo‘lmagan holatlar anomal hodisalar deb ataladi.

Boshqacha qilib aytganda, anomal insident - bu himoya vositasi tomonidan belgilangan sinf ichidagi analoglari bo‘lmagan insident. Buni yodda tutgan holda, hodisa tahlillar topilgan analogiyalar soniga qarab, hodisalarning oddiy va anomalga bo‘linishini anglatadi:

$G = \{g_1, \dots, g_n\}$ – ko‘plab hodisalar; $g_i = (x_1, \dots, x_p, r_i)$ – bir martalik hodisa; $K = \{k_1, \dots, k_m\}$ – ko‘plab qayd qilingan insidentlar; $k_j = \{x_1, \dots, x_p\}$ – bir martalik insident; $F(g_i, k_j)$ – mutanosiblik funksiyasi; $G_1 = \{g_i : F(g_i, k_j) \le d_{lim}\}$ – ko‘plab mutanosib hodisalar.



19- rasm. Pretsedent tahlil qilish tizimining mantiqiy tuzilishi

Shunday qilib, insidentni ko‘lab hodisalarga bog‘lash quyidagi ifodada aks etadi: $k_j \in G \leftrightarrow |G_1| \geq a_{lim}$

Ko‘rib turganimizdek, tasniflash natijasi bevosita d_{lim} eng yuqori masofasi va a_{lim} hodisalarning eng ko‘p soniga bog‘liq.

Hodisa tahlili algoritmining modeli. Metrik klassifikator sifatida k - yaqin qo‘shnilar usuli qo‘llaniladi. Algoritmning tajriba ssenariysi Deductor Studio Academic analitik platformasida ishlab chiqilgan va o‘z ichiga quyidagi bosqichlarni oladi (20- rasm):

Insident qayd etilganidan so‘ng, u normallashtiriladi:

$$x_{norm} = \frac{x - x_{min}}{x_{max} - x_{min}}.$$

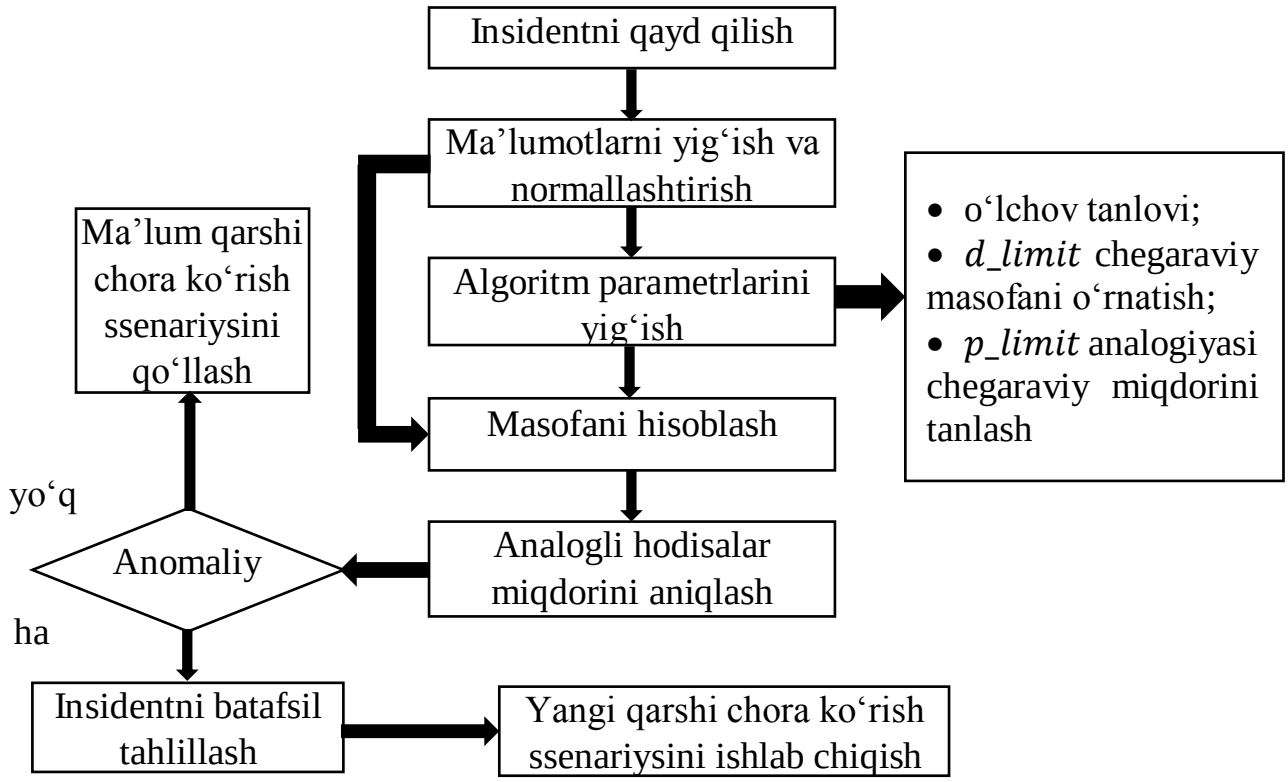
1. Algoritm parametrlarini aniqlashtirish: metrikani tanlash, d_{lim} eng yuqori masofasi va eng a_{lim} katta qiymatni aniqlash. d_{lim} Boshlang‘ich qiymat sifatida sinfdagi masofa qabul qilingan. Bunda bir martalik hodisaning sinfgacha o‘rtacha masofasi quyidagiga teng

$$d_{cp} = \frac{\sum_{i=1}^{n} d_{i_{cp}}}{n}$$

2. Obyektlar orasidagi masofani o‘lchovlar quyidagi metrika bo‘yicha amalga oshiriladi

$$d_{i_{cp}} = \sqrt{\sum_{i=1}^{p}(x_{gi} - x_{ki})^2}.$$

3. $d_{gk} \leq d_{lim}$ ifodasi taalluqli bo‘lgan obyektlar juftligini topish(g hodisa va k insident o‘xshash deb olinadi)



20- rasm. Boshqarish jarayoniga insidentlar tahlilini kiritish

4. k_j insident uchun a hodisa soni hisoblanadi, buning uchun

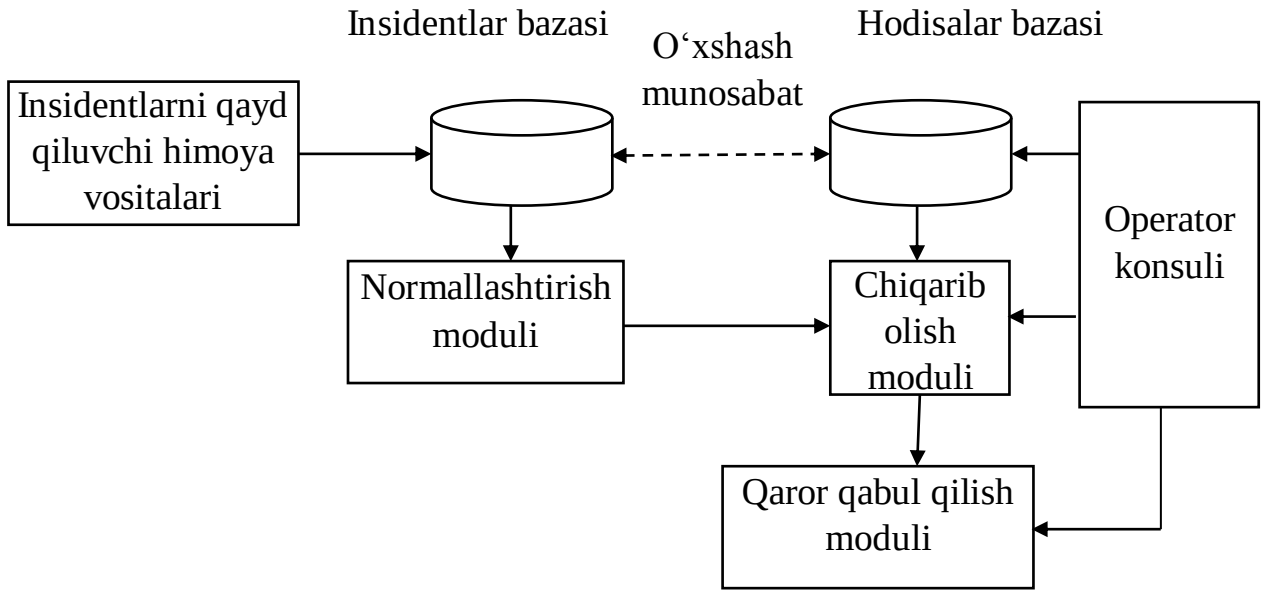
$$d_{gk} \leq d_{lim}.$$

bajariladi.

5 . k_j Insidentlar $a \leq a_{lim}$ bo‘lganda anomaliya deb hisoblanadi

6. Klassifikatsiyalash natijalari bo‘yicha qo‘shimcha harakatlar amalga oshiriladi: insidentlarni batafsil tahlil qilish yoki eng ko‘p o‘xshash holatga mos keladigan javob berish harakatlar strategiyasidan foydalanish. Algoritm parametrlari tizimning ishlashi vaqtida o‘zgarib turadi, shuning hisobiga, tizim hodisalarining bazalarini to‘ldirish bilan birga ta’lim oladi.

Pretsedent tahlili tizimining arxitekturasi. Dasturiy ta’minot amalga oshirish nuqtai nazaridan hodisa tahlili tizimi modul tuzilishiga ega va o‘z ichiga quyidagi birliklarni oladi (21- rasm):



21- rasm. Pretsedent tahlili tizimi arxitekturasi

1) kelgusida ishlov berishni kutayotgan insident yozuvlarini o‘z ichiga olgan ma’lumotlar bazasi;
2) ro‘yxatga olingan insidentlarning bazasini pretsedentlarning tuzilishiga mos ravishda o‘zgartiruvchi ma’lumotlarning normallashuv moduli;
3) klassifikatsiya natijasini aniqlovchi va mutanosiblik choralariga asosan insidentni bir yoki bir necha hodisaga qo‘yuvchi qaror qabul qilish moduli;
4) ishlab chiqilgan strategiyani oldindan noma’lum sharoitlarga moslashtirish va tahlil jarayonini tuzatish uchun mo‘ljallangan operator konsoli.

Shunday qilib, axborot xavfsizligi insidentlarini boshqarish jarayonini takomillashtirish vositasi sifatida pretsedent tahlili konsepsiyasini qo‘llash to‘plangan tajribadan takroran foydalanish orqali sodir bo‘lgan insidentlarga javob ko‘rsatish tezligini oshiradi. Bundan tashqari, ushbu yondashuv eng muhim bo‘lgan va batafsil o‘rganishni talab qiluvchi anomal hodisalarni aniqlash bilan bog‘liq muammolarni hal qilishga imkon beradi.

4.6. Raqamli steganografiya

Ma’lumotni ruxsatsiz kirishdan himoya qilish vazifasi insoniyat tarixi davomida har doim ham hal qilinib kelingan. Qadimgi dunyoda allaqachon mavjud bo‘lgan ushbu muammoni hal etishning ikki asosiy yo‘nalishi mavjud edi. Axborotni himoya qilish uchun ko‘plab usullar va algoritmlar allaqachon ixtiro qilingan bo‘lib, ularni ikki yo‘nalishdan biriga kiritish mumkin: kriptografiya, steganografiya.

Kriptografiyaning maqsadi - xabarlarning mazmunini ularni shifrlash orqali yashirishdir. Buning teskari ravishda, steganografiyada maxfiy xabarning borligi yashiriladi.

"Steganografiya" so‘zi yunon tilidan olingan bo‘lib, so‘zma-so‘z **"maxfiy yozish"** degan ma’noni anglatadi. Tarixiy jihatdan kriptografiyadan oldin steganografiya ma’lumotlarni yashirish yo‘shnalishi paydo bo‘lgan. Shu bilan birga, vaqt o‘tishi bilan bu sohada tadqiqotlar sezilarli darajada kamaydi va bu fan ko‘plab sohalarda kriptografiya tomonidan chiqarilib yuborildi. Yashirin yozish turli usullar bilan amalga oshiriladi. Ushbu usullarning umumiy xususiyati shundaki, yashiringan xabar ba’zi zararsiz, ko‘zga tushmaydigan obyektga singdiriladi. Keyin ushbu obyekt manzilga ochiq yuboriladi. Kriptografiyada shifrlangan xabarning o‘zi raqiblarning e’tiborini tortadi, steganografiyada esa, yashirin aloqaning mavjudligi sezilmay qoladi.

Hisoblash vositalarining rivojlanishi so‘nggi o‘n yil ichida kompyuterni rivojlantirishga yangi turtki berdi. Ko‘pgina yangi dasturlar paydo bo‘ldi. Xabarlar endilikda raqamli ma’lumotlarga, odatda, analog tabiatiga xoslariga kiritiladi. Ular sirasiga nutq, audio yozuvlar, tasvirlar, videolar kiradi.

Steganografiya aslida aloqaning mavjudligini yashiradigan aloqa vositasidir. Raqib yuborilgan xabarning shifrlangan matnni aniq-ravshan belgilashi mumkin bo‘lgan kriptografiyadan farqli o‘laroq, steganografiya usullari maxfiy xabarlarni zararsiz axborotga shunday joylash imkonini beradiki, yashirin maxfiy xabar borligi to‘g‘risida shubha uyg‘onmaydi.

Steganografik texnika axborot yashirish sohasidagi umumiy yo‘nalishning bo‘limlaridan biri. Steganografiyada ma’lumotlarni yashirishni o‘rganuvchi boshqa yo‘nalishlar ham mavjud. Bu kriptografiya, turli signalizatsiya tizimlari va shartli belgilar, niqoblash va chalkashtirish, nihoyat, bir xil so‘zlarning turli talqinlari va h.k.

Steganografiyaning bir necha yo‘nalishlari ajratilgan:

– klassik steganografiya;
– kompyuter steganografiyasi;
– raqamli steganografiya.

Klassik stanografiya kompyuterdan foydalanmasdan xabarni yashirishning turli usullarini anglatadi va odatda murakkab texnik vositalarsiz foydalanadi.

Bugungi kunda klassik steganografiya uzatiladigan va saqlanadigan hujjatlardagi axborotni yashirishning turli xil usullarini qo‘llaydi. Ularga ko‘rinmas siyoh, mikronuqtalar, akrostik, trafaretlar va boshqalar kiradi.

Kompyuter steganografiyasi turli xil fayllar, dasturlar, protokol paketlari va shunga o‘xshash bo‘lgan kompyuter ma’lumotlarini yashirish usullarini o‘rganadi. Inson faoliyatining barcha sohalarining umumiy kompyuterlashtirilishini hisobga olgan holda, hozirgi kunda raqamli va kompyuterli steganografiya o‘rtasidagi farqni aniqlash juda qiyin. Aloqa tizimlarida analog signallar (audio, video) paketlarga bo‘lingan va tarmoq orqali uzatiladigan diskret ketma-ketliklar yoki oqimlar shakllariga aylantirilgani kabi, rasmlar, tovush yoki videoga mos keladigan kompyuter ma’lumotlari kompyuter tarmog‘i orqali fayllar sifatida yoki paketlar sifatida uzatiladi.

Quyida ba’zi misollar keltirilgan:

– Format fayldagi zahira maydonidan foydalanish- usulning mohiyati shundaki, kengaytma to‘g‘risidagi ma’lumot bilan to‘ldirilmagan fayl qismi nollar bilan avtomatik ravishda to‘ldiriladi. Bundan kelib chiqib, biz ushbu “nolli” maydonni o‘z ma’lumotlarimizni yozish uchun qo‘llashimiz mumkin. Bu usulning kamchiligi shundaki, yashirish darajasining pastligi va kam miqdordagi axborot uchun mo‘ljallanganligi.

– Yumshoq disklarning foydalanilmagan qismida axborotni yashirish usuli - bu usuldan foydalanganda ma’lumot diskning foydalanilmagan qismlarida, masalan, nolinchi yo‘lakda saqlanadi. Kamchiliklari: past samaradorlik, kichik xabarlarni yetkazish.

– Ekranda aks ettirilmagan format maydonlarining maxsus xususiyatlaridan foydalanish usuli - maxsus izohlar va ko‘rsatmalarni olish uchun mo‘ljallangan "ko‘rinmas" joylarga asoslangan usuldir. Masalan, qora fonda qora yozish. Kamchiliklari: past unumdorlik, uzatiladigan ma’lumotlarning oz miqdori.

– Fayl tizimining funksiyalaridan foydalanish - qattiq diskda saqlanganida, fayl har doim klasterlarning to‘liq sonini egallaydi. Misol uchun, ilgari keng ishlatiladigan FAT32 fayl tizimida klasterini standart hajmi – 4 KB. Shunga mos ravishda, diskda 1 KB axborotni saqlash uchun 4 kilobayt xotira ajratilgan, ulardan 1 kilbayt faylni saqlash uchun kerak, qolgan 3 esa hech narsaga ishlatilmaydi - ular ma’lumotni saqlash uchun ishlatilishi mumkin. Ushbu usulning kamchiligi: aniqlashni osonligi.

Raqamli steganografiya - raqamli obyektlarga qo‘shimcha ma’lumotni yashirish yoki kiritishga asoslangan klassik steganografiyaning yo‘nalishi hisoblanadi, shu bilan birga u ushbu obyektlarning bir qismini buzadi. Lekin, odatda, ushbu obyektlar multimediya obyektlari bo‘lib, oddiy shaxsning sezgirlik chegarasidan past bo‘lgan buzilishlarni joriy qilish bu obyektlardagi sezilarli o‘zgarishlarga olib kelmaydi. Bundan tashqari, dastlab analog tabiatda joylashgan raqamli moslamalarda, doimo kvantlash shovqini mavjud; keyinchalik, ushbu obyektlar ishga tushirilganda, qo‘shimcha analog shovqin va uskunaning noan’anaviy buzilishlari paydo bo‘ladi, ularning hammasi maxfiy axborotning yuqori darajadagi ko‘rinmasligiga yordam beradi.

Tarmoq steganografiyasi. So‘nggi paytlarda maxfiy axborot uzatish protokollarining xususiyatlaridan foydalangan holda kompyuter tarmoqlari orqali axborot uzatish usullari keng qo‘llanilmoqda. Bunday usullarga tarmoq steganografiyasi deb ataladi. Tarmoq steganografiyasi uchun odatiy usullar tarmoq protokollaridan biri xususiyatlarini o‘zgartirishni o‘z ichiga oladi. Bundan tashqari, yashirin xabarni uzatishni yanada xavfsizroq qilish uchun ikki yoki undan ortiq turli protokollar orasidagi o‘zaro bog‘liqlikdan foydalanish mumkin. Tarmoq steganografiyasi keng ko‘lamdagi usullarni o‘z ichiga oladi, xususan:

– **WLAN-steganografiya** stenogrammani simsiz tarmoqlarga (simsiz mahalliy tarmoqqa) uzatish uchun ishlatiladigan usullarga asoslangan (Wireless Local Area Networks). WLAN - steganografiyaning amaliy namunalari – bu HICCUPS (Hidden Communication System for Corrupted Networks) tizimi.

– **LACK-steganografiya** - IP-telefoniya orqali suhbatlar paytida xabarlarni yashirish. Misol uchun, kechiktirilgan yoki qasddan shikastlangan va qabul qiluvchi tomonidan e’tiborsiz bo‘lgan paketlarni ishlatish (bu uslub LACK - Lost Audio Packets Steganography deb

ataladi) yoki foydalanilmaydigan ustunli maydonlarda ma’lumotlarni yashirish.

Hozirgi kunda kompyuter steganografiyasi usullari ikki asosiy yo‘nalishda rivojlanmoqda:

1. Kompyuter formatlarining maxsus xususiyatlaridan foydalanishga asoslangan usullar;
2. Audio va vizual axborotning ortiqcha bo‘lishiga asoslangan usullar.

Birinchi usul ma’lumotlarning ko‘pligiga emas, ma’lumotlarni taqdim etish formatlarining maxsus xususiyatlariga asoslangan. Formatlarning maxsus xususiyatlari to‘g‘ridan-to‘g‘ri tinglash, ko‘rish yoki o‘qishdan maxfiy xabarni himoya qilishga asosan tanlanadi. Kompyuter steganografiyasining asosiy yo‘nalishi - bu ortiqcha audio va vizual axborotdan foydalanish. Raqamli fotosuratlar, raqamli musiqa, raqamli video - makon va/yoki zamonning turli nuqtalarida zichlikni kodlovchi raqamlar matritsalari bilan ifodalanadi. Raqamli fotosurat - ma’lum bir nuqtada yorug‘likning intensivligini ifodalovchi raqamlarning matritsasi. Raqamli tovush- ketma-ketlikda ovozli signalning intensivligini aks ettiradigan raqamlar matritsasidir. Bu sonlarning barchasi noaniqdir, chunki analog signallarni raqamlash uchun moslamalar aniq ishlamaydi, kvantlash shovqinlari mavjud. Raqamli hisobotning quyi darajadagi vakillari tovush va vizual tasvirning joriy parametrlari haqida juda kam foydali ma’lumotlarni o‘z ichiga oladi. Ularni to‘ldirish ma’lumotni idrok etish sifatiga sezilarli ta’sir ko‘rsatmaydi, bu qo‘shimcha axborotni yashirish imkonini beradi.

Steganografik tizim yoki **stegotizim** axborotni uzatish maqsadida maxfiy kanal yaratish uchun ishlatiladigan vositalar va usullar to‘plami.

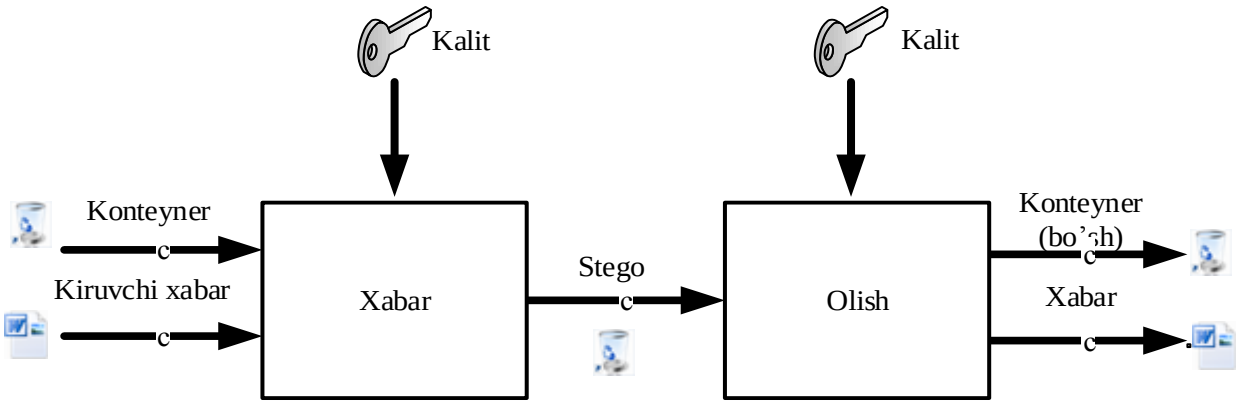
Steganosistemani qurishda quyidagi qoidalar e’tiborga olinishi kerak:

– raqib steganografik tizim va uni amalga oshirish tafsilotlarini to‘liq biladi. Potensial raqibga noma’lum bo‘lgan yagona ma’lumot, bu faqat uning egasi mavjudligi va maxfiy xabarning mazmunini belgilashi mumkin bo‘lgan kalit;

– agar raqib maxfiy xabar mavjudligini bilib olsa, u kalitga ega bo‘lmaguncha, boshqa ma’lumotlarda saqlanuvchi o‘xshash xabarlarni olishiga yo‘l qo‘ymaydi;

– potensial raqib maxfiy xabar tarkibini ochishda texnik va boshqa ustunliklarga ega bo‘lmasligi lozim.

Steganotizimning umumiy modeli 22- rasmda keltirilgan.



22- rasm. Steganotizimning umumlashtirilgan modeli

Har qanday ma’lumot axborot sifatida ishlatilishi mumkin: matn, xabar, rasm va hokazo. Umuman olganda, "xabar" so‘zidan foydalanish tavsiya etiladi chunki, xabar matn, tasvir yoki audio ma’lumot bo‘lishi mumkin. Keyinchalik, maxfiy axborotni ifodalash uchun, biz xabar so‘zini ishlatamiz.

Konteyner - maxfiy xabarlarni yashirishga mo‘ljallangan har qanday ma’lumot.

Bo‘sh konteyner - singdirilgan xabarga ega bo‘lmagan konteyner; to‘ldirilgan konteyner yoki stego - singdirilgan ma’lumotni o‘z ichiga olgan konteyner.

Kiruvchi (maxfiy) xabar - konteynerga biriktirilgan xabar.

Steganografik kanal yoki oddiygina stegokanal - stegoni uzatish kanali.

Stego kaliti yoki shunchaki kalit - ma’lumotlarni yashirish uchun zarur bo‘lgan maxfiy kalit. Himoya darajalarining soniga (masalan, oldindan shifrlangan xabarlarni joylashtirishga) qarab steganosistemada bir yoki bir necha stegokalit bo‘lishi mumkin.

Kriptografiyaga mos ravishda, steganosistemani stegokalitga asosan ikki turga bo‘lish mumkin:

– maxfiy kalit bilan;

– ochiq kalit bilan.

Yashirin kalitli steganosistemada, bir kalit ishlatiladi, bu maxfiy xabarlar almashinuv boshlanishidan oldin yoki xavfsiz kanal orqali uzatilishi kerak.

Ochiq kalitli steganosistemasida xabarni joylash yoki olish uchun turli xil kalitlardan foydalaniladi, ularni hisob-kitoblarni qo‘llash orqali bir-biridan ajratish va farqlashning ilojisi yo‘q. Shuning uchun, bir kalit (ommaviy) himoyalanmagan aloqa kanali orqali erkin uzatilishi mumkin. Bundan tashqari, ushbu sxema jo‘natuvchi va qabul qiluvchining o‘rtasida ishonchsizlik mavjudligida yaxshi ishlaydi.

Raqamli steganografiya ilmiy jihatdan so‘nggi yillarda paydo bo‘ldi. Bizning fikrimizcha, u quyidagilarni o‘z ichiga oladi:

1) yashirin uzatish maqsadida ma’lumotlarni joylashtirish;
2) raqamli suv belgilarini kiritish (watermarking);
3) identifikatsiya raqamlarini kiritish (fingerprinting);
4) sarlavhalarni joylashtirish (captioning).

4.7. Raqamli suv belgilari

Raqamli suv belgilari (RSB) asosan nusxa ko‘chirish va ruxsatsiz foydalanishdan himoyalash uchun ishlatilishi mumkin. Multimediya texnologiyalarining jadal rivojlanishi munosabati bilan raqamli shaklda taqdim etilayotgan mualliflik va intellektual mulkni himoya qilish masalasi keskinlashdi. Masalan, fotosuratlar, audio va video yozuvlar va boshqalar. Raqamli ko‘rinishda xabarlarni taqdim qilish va yetkazishning afzalliklari ularning o‘g‘irlanishi yoki o‘zgartirilishi mumkin bo‘lgan qulaylik bilan kesishadi. Shu sababli, tashkiliy va texnik jihatdan axborotni himoya qilish bo‘yicha turli tadbirlar ishlab chiqilmoqda. Multimediali axborotni muhofaza qilishning eng samarali texnik vositalaridan biri ko‘zga ko‘rinmas belgilardan foydalanish, ya’ni RSBni himoyalangan obyektga kiritishdir. Ushbu sohadagi izlanishlarni dunyodagi eng yirik kompaniyalar olib bormoqda.

Raqamli steganografiya tavsifida "sezilmas" so‘zi odamni steganografik ma’lumotlarni uzatish tizimiga majburiy kiritishni nazarda tutadi. Insonga bu yerda qo‘shimcha ma’lumotni qabul qiladigan, uzatish tizimiga bajarilishi ancha qiyin bo‘lgan masalalarni qo‘yadigan shaxs sifatida qaralishi mumkin.

Prekoder - yashirin xabarni signal - konteynerga joylashtirish uchun qulay bo‘lgan formaga aylantirish uchun mo‘ljallangan qurilma. (Konteyner deb ma’lumot ketma-ketligiga yashiringan xabar tushuniladi).

Stegokoder - xabarning modelini inobatga olgan holda boshqa ma’lumotlarda maxfiy xabarni joylashtirish uchun mo‘ljallangan qurilma.

Stegodetektor - stego xabarning mavjudligini aniqlash uchun mo‘ljallangan qurilma.

Dekoder - yashiringan xabarni tiklaydigan qurilma.

Stegodetektorda RSB tomonidan himoyalangan suratdagi RSB aniqlanadi. Ushbu o‘zgarish aloqa kanalidagi xatolar, signalni qayta ishlash amaliyotlari, buzg‘unchilarning qasddan hujumlari ta’sirida bo‘lishi mumkin. Steganosistemalarning ko‘plab modellarida signal-konteyner qo‘shimchali shovqin hisoblanadi. Bu holda stego xabarlarni aniqlash va izolyatsiya qilish vazifasi aloqa nazariyasi uchun klassikdir. Biroq bu yondashuv ikki omilni hisobga olmaydi: konteyner signalining tasodifiy xarakteri va uning sifatini saqlab qolish talablari. Bu holatlar qo‘shimcha shovqin fonida signalni aniqlash va ajratib olishning ma’lum nazariyasida uchramaydi. Ularni hisobga olish yanada samarali steganosistemalarni yaratish imkonini beradi.

RSB mavjudligini va vositani aniqlashga, ushbu RSB ni ajratib olishga (stegodekoder) mo‘ljallangan stegodekoderlar turlari mavjud. Birinchi holda qattiq yoki yumshoq yechimlarga ega detektorlar bo‘lishi mumkin. RSB ning mavjudligi / yo‘qligi qulay aniqlash uchun uchun Hemming bo‘yicha masofa yoki mavjud va original signal o‘rtasidagi o‘zaro bog‘liqlik usullarini qo‘llash qulay. Agar asl signal mavjud bo‘lmasa-chi? Bunda sinchkovlik bilan o‘rganilayotgan signal sinflarining modellarini qurish asosida yanada nozik statistika usullari qo‘llanadi

Konteyner tushunchasini batafsil ko‘rib chiqaylik. S*tegokodergacha* – bu bo‘sh konteyner, undan so‘ng - to‘ldirilgan konteyner yoki stego. Stego bo‘sh konteynerdan ko‘rinishidan farq qilmasligi kerak. Ikki asosiy konteyner turi mavjud: *oqim va turg‘un*.

Oqim konteyneri uzluksiz bit ketma-ketligidir. Xabar real vaqtda o‘rnatiladi, shuning uchun kodlovchi konteyner barcha xabarni yetkazish uchun yetarlicha hajmga ega bo‘ladimi-yo‘qmi oldindan noma’lum. Bir nechta xabarlar bitta katta konteynerga joylangan bo‘lishi mumkin. Joylangan bitlar orasidagi interval psevdotasodifiy generator yordamida aniqlanadi va hisoblar orasida intervallar teng bo‘linadi.

Turg‘un konteynerda o‘lchovlar va xususiyatlar oldindan ma’lum. Bu ma’lumotlarning eng yaxshi tarzda joylashtirilishiga imkon beradi.

Konteyner tanlangan, tasodifiy yoki belgilangan bo‘lishi mumkin. Tanlangan konteyner joylangan xabarga bog‘liq va cheklangan holda uning funksiyasi hisoblanadi. Bu konteyner turi steganografikaga xosdir. Konteynerni taqdim etuvchi shaxs yashirin yozishmalarning mavjudligidan shubha ostiga qo‘yishi va uni oldini olishni xohlagan payt belgilangan konteyner paydo bo‘lishi mumkin. Amaliyotda ko‘pincha tasodifiy konteyner bilan ko‘proq duch kelinadi.

RSB uch turda bo‘lishi mumkin: *baquvvat, nozik va yarim nozik (semifragile)*.

Baquvvatlik deganda bu tizimda turli ta’sirlarga nisbatan katta chidamlilikka ega bo‘lish nazarda tutilgan.

Nozik RSB to‘ldirilgan konteynerning yengil o‘zgarishi bilan yo‘q qilinadi. Ular signallarni tasdiqlashda foydalaniladi. Elektron raqamli imzo vositalaridan farqi shundaki, nozik ESB tarkibni o‘zgartirishga ruxsat beradi. Bu multimediali axborotni muhofaza qilishda muhimdir, chunki qonuniy foydalanuvchi, masalan, rasmni siqishni xohlashi mumkin. Yana bir farq shundaki, nozik RSBlar konteyner o‘zgartirilishining asl holatidan tashqari, bu o‘zgarishning turi va joylashuvini ham aks ettirishi kerak.

Yarim nozik RSBlar ba’zi ta’sirlarga nisbatan barqaror va boshqalarga nisbatan beqaror. Odatda, barcha RSBlar ushbu turga bog‘liq bo‘lishi mumkin. Shu bilan birga, yarim nozik raqamli shiftlar muayyan turdagi operatsiyalarga nisbatan beqaror bo‘lishi uchun maxsus mo‘ljallangan. Misol uchun, ular rasmni siqishni bajarishga ruxsat berishlari mumkin, lekin uni kesib olishni yoki unga qismni kiritishni taqiqlaydi.

Muhim muammo - olingan ma’lumotlarning haqiqiyligini aniqlash, ya’ni uning autentifikatsiyasidir. Odatda, ma’lumotlarni autentifikatsiya qilish uchun raqamli imzoni qo‘llaniladi. Biroq bu vositalar multimedia autentifikatsiyasini ta’minlash uchun mutlaqo mos emas. Negaki, raqamli imzo bilan yozilgan xabar "bitdan bitgacha" aniq saqlanishi va yetkazilishi kerak. Multimedia ma’lumotlarini saqlash paytida (siqilish sababli) va uzatish paytida (kanalda bitta yoki paketli xatolikning ta’siri) birmuncha buzilishi mumkin. Bunda uning sifati foydalanuvchi uchun to‘liqligicha saqlanadi, ammo raqamli imzo ishlamaydi. Qabul qiluvchi haqiqatni biroz buzilgan noto‘g‘ri ma’lumotlardan ajratib olishining iloji

yo‘q. Bundan tashqari, multimedia ma’lumotlari bir formatdan ikkinchisiga aylantirilishi mumkin.Shu bilan birga, an’anaviy yaxlitlikni himoya qilish vositalari ham ishlamaydi. Aytish kerakki, RSB audio-video xabarining mazmunini himoya qiladi, lekin uning raqamli tasviri bitlar ketma-ketligi shaklini emas. Bundan tashqari, raqamli imzoning muhim kamchiliklaridan biri, tasdiqlangan xabardan olib tashlash va unga yangi imzo qo‘yish osondir. Imzoni o‘chirib tashlash huquqbuzarning mualliflik huquqidan voz kechishiga yoki huquqiy oluvchini xabar muallifligiga nisbatan chalg‘itishga imkon beradi. Ma’lumotni himoya qilish uchun suv belgilarini qo‘llashning asosiy yo‘nalishlarini ko‘rib chiqamiz:

1. Keng uzatishli nazorat.
2. Egalik qiluvchi shaxsni identifikatsiyalash.
3. Mulkka egalik huquqining isboti.
4. O‘zaro faoliyatni kuzatish
5. Ma’lumotlarni autentifikatsiya qilish.
6. Noqonuniy nusxalashni boshqarish.
7. Qurilmalarni boshqarish
8. Turli texnologiyalarning mosligi.

Keng uzatishli nazorat. Radioeshittirishda muhim rol o‘ynaydi. Misol uchun, 1997 yilda Yaponiyada televizion reklamalarni tarqatish haqida janjal kelib chiqdi. Reklama beruvchilar televizion stansiyalarda efirga uzatilmagan reklamalarni namoyish etish uchun pul to‘lashdi. Bu reklama beuvchining aldovi 20 yildan ko‘proq vaqt davom etdi, chunki reklama uzatishni boshqaruv tizimlari mavjud emas edi.

Eshittirishni boshqarishning ikkita asosiy turini ko‘rib chiqaylik: passiv va faol nazorat qilish tizimlari:

– Faol nazorat qilish tizimlari axborot tarkibi bilan birga eshittiriluvchi ma’lumotning mutanosibligini tekshiradi;

– Passiv boshqaruv tizimlari dasturlarning mazmunini aniqlash yo‘li bilan amalga oshiriladi.

Keling, ushbu ikki turdagi farqlarni tahlil qilaylik. Passiv boshqaruv tizimlarida kompyuter efirni boshqarish jarayonini amalga oshiradi. Ushbu jarayon davomida olingan taniqli teleko‘rsatuvlar, filmlar, qo‘shiqlar va h.klarni o‘z ichiga olgan signallarni ma’lumotlar bazasi bilan taqqoslash mumkin. Agar o‘xshashlik topilsa, ma’lumot (film, reklama, va hokazo) identifikatsiyalanadi va efirga uzatiladi.

Passiv boshqaruv tizimlari o‘zlarining kamchiliklariga ega. Kompyuterning kiruvchi signal va ma’lumotlar bazasi o‘rtasidagi

o‘xshashlikni aniqlash jarayoni ahamiyatsiz emas. Shuni ta’kidlash joizki, uzatishning o‘zi uni yomonlashtirishi mumkin. Shuning uchun bunday monitoring tizimi uzatish va ma’lumotlar bazasi o‘rtasidagi aniq moslikni aniqlay olmaydi. Ma’lumotlar bazasida qidirish jarayonini izga solish amalga oshsa ham, katta hajm tufayli uni saqlash va boshqarish qimmatga tushishi mumkin. Ta’kidlash joizki, kompaniyalar yetarlicha aniq tan olinmaganligi sababli passiv boshqaruv tizimlaridan foydalanmaydi. Endi passiv tizimlarga qaraganda amalga oshirish oson bo‘lgan faol nazorat qilish tizimlarini ko‘rib chiqing. Ushbu usulda kompyuter identifikatsiya ma’lumotlarini tarkib bilan birga uzatadi, bunday boshqaruv tizimini qo‘llash uchun identifikatsiya ma’lumotlari uzatilgan signalning alohida maydoniga joylashtiriladi. Ushbu usulda ham kamchiliklar mavjud. Masalan, signalga qo‘shimcha ma’lumotlar qo‘shganda, uning formatini analogdan raqamligacha o‘tishga dosh bermasligi mumkin. Ushbu o‘zgartirishlar ularni amalga oshiradigan maxsus apparatni talab qiladi. Ushbu muammoni hal qilish uchun identifikatsiya ma’lumotlarini kodlashning muqobil usuli mavjud - bu suv belgilaridir. Ular translyatsiya segmentini ishlatmasdan tarkib ichida bo‘lishi mumkin. Ushbu usulning muhim afzalligi shundaki, suv belgilari analog va raqamli translyatsiyalarni o‘z ichiga oladigan uzatish uskunalari bilan to‘liq mos keladi. Shu bilan birga, bu uslubning o‘z kamchiliklari ham bor. Suv belgisini qo‘llash qo‘shimcha ma’lumotlarni joylashtirishdan ko‘ra murakkabroqdir. Bundan tashqari, filtrlar uzatilgan ma’lumotlarning sifatiga ta’sir qilishi mumkin, masalan, audio yoki video ma’lumotlarining sifati yomonlashishiga olib kelishi mumkin.

Egalik qiluvchi shaxsni identifikatsiyalash. Ko‘pgina original ma’lumotlar mualliflari faqat matnli mualliflik huquqi eslatmalaridan foydalanadilar, ammo ularni qasddan va bilmasdan osongina olib tashlash mumkin deb o‘ylamaydilar. Keyinchalik ushbu ma’lumotlar masofaviy mualliflik huquqi bilan qonunga amal qiladigan fuqaroga yetib kelishi mumkin va u bu ma’lumotlarda mualliflik huquqi bor yoki yo‘qligini aniqlay aniqlay olmaydi. Mualliflik huquqini o‘rnatish jarayoni juda mashaqqatli va muallifni topish har doim ham amalga oshmaydi. Mualliflik huquqini himoya qilish muammosini hal qilish uchun suv belgilaridan foydalaniladi, chunki ular ko‘rinmas va ma’lumotlar bilan uzviy bog‘liqdir. Bunday holda, muallif shu maqsadda mo‘ljallangan detektorlardan foydalangan holda, suv belgilarini osongina aniqlanadi.

Mulkka egalikning tasdiqlanishi. Buzg‘unchi biron bir ma’lumotning egasi bo‘lishni talab qilish uchun boshqa birovning suv belgilaridan foydalanishi mumkin. Bunday holatlarning oldini olish uchun detektorning qo‘llanilishini cheklash kerak. Detektorga ega bo‘lmagan buzg‘unchining suv belgisini olib tashlay olmaydi, chunki bu oson ish emas.

O‘zaro aloqani kuzatish. Bu turning mohiyati quyidagicha: ma’lum ma’lumotlarga tegishli suv belgisi nusxa ko‘chirish sonini qayd etib, har bir nusxani bittadan aniqlaydi. Misol uchun, har qanday ma’lumot egasi har bir nusxada turli xil suv belgilarini qo‘yadi va agar ma’lumotlar tarqalishi sodir bo‘lsa, aybdor kim ekanligini aniqlay oladi.

Ma’lumotlarni autentifikatsiya qilish. Ma’lumotlarning haqiqiyligini himoya qilish uchun shifrlangan xabar mavjud bo‘lgan raqamli imzolardan foydalaniladi. Faqat mualliflik huquqi egasi bunday imzo yaratish uchun zarur kalitni biladi. Bunday imzolarning kamchiligi -ishlatilish vaqtida yo‘qolishdir. Keyin raqamli haqiqiyligi bo‘lmagan ish haqiqiylik sinovidan o‘ta olmaydi. Ushbu muammoni hal qilish to‘g‘ridan-to‘g‘ri suv belgisi himoyalovchi ma’lumotlarga imzo qo‘yishdir. Bunday joylangan imzolar autentifikatsiya belgisi deb ataladi. Mualliflik huquqi egasi ma’lumotni o‘zgartirsa, autentifikatsiya belgisi u bilan o‘zgartiriladi. Ushbu funksiya yordamida ma’lumotni qanday qilib soxtalashtirishga urinayotganini aniqlash mumkin. Misol uchun, tadqiqotchilar bunday fikrni o‘rtaga tashladilar: agar tasvirni bloklarga bo‘lib, ularning har biriga alohida suv belgisiga joylansa, tasvirning qaysi fragmetlarni o‘zgartirilgan qaysilari o‘z holicha qolganini aniqlash mumkin.

Noqonuniy nusxalashni nazorat qilish. Suv belgilarini qo‘llashning yuqorida ko‘rsatilgan usullari faqat huquqbuzar tomonidan sodir etilgan har qanday xatti-harakatdan so‘ng kuchga kiradi. Ushbu texnologiyalar jinoyatchini faqat noqonuniy xatti-harakatlar qilinganidan keyin aniqlash imkonini beradi. Shu sababli, ushbu tur huquqbuzarning muallifga qarashli mualliflik huquqi bilan himoyalangan ma’lumotlarni noqonuniy nusxasini olishiga to‘sqinlik qilishi mumkin bo‘lgan boshqa texnologiyani nazarda tutadi. Noqonuniy nusxalashga qarshi eng yaxshi nazoratni ma’lumotlarni o‘zida joylashgan suv belgilarini berishi mumkin.

Qurilmani boshqarish. Foydalanuvchilarning fikriga ko‘ra, ushbu tur yuqorida muhokama qilinganlardan farq qiladi, chunki u ma’lumotlarni yangi xususiyatlar bilan to‘ldiradi va ulardan

foydalanishni cheklamaydi. Bu turdan foydalanishning bir misolini ko‘rib chiqaylik. Digimarc’s Mobile System kompaniyasi tomonidan gazeta, jurnal, e’lonlar va boshqalar ishlatiladigan tasvirlarga noyob identifikatorlarni joylashtirish taklif qilindi. So‘ngra, foydalanuvchi ushbu tasvirga telefon kamerasini qaratib, maxsus dastur yordamida tasvirning suv belgisini aniqlaydi. Identifikator o‘z navbatida telefonning veb-brauzerini tegishli saytga yo‘naltiradi.

Turli texnologiyalarning mosligi. Har qanday katta tizimlar foydalanuvchilari ba’zan yaxshilangan funksiyalarni olish uchun ularni yangilashlari kerak. Ammo, yangilash eski tizim bilan mos kelmasligi mumkin. Ikki xil tizimning muvofiqligi muammosini hal qilish va hamkorlikni davom ettirish uchun raqamli suv belgilaridan foydalaniladi.

4.8. Yashirin xabarlar uzatish tizimlariga qarshi hujumlar

Steganosistemalarga qarshi hujumlar quyidagi toifalarga ajratilishi mumkin:

1. ***O‘rnatilgan xabarga qarshi hujumlar*** - stegoni o‘zgartirish orqali RSBni yo‘q qilish yoki zarar yetkazishga qaratilgan. Ushbu turkumdagi hujum usullari suv belgisini baholashga va aniqlashga urinmaydi. Bunday hujumlarga, masalan, chiziqli filtrlash, tasvirni siqish, shovqin qo‘shilishi, gistogramlarni joylashtirish, kontrastni o‘zgartirish va boshqalar kirishi mumkin.
2. ***Stegodetektorga qarshi hujum*** - detektorning to‘g‘ri ishlashini qiyin yoki imkonsiz qilish uchun mo‘ljallangan. Bunday holda rasmdagi suv belgisi qoladi, lekin uni qabul qilish ehtimoli yo‘qoladi. Ushbu turkumda affinli o‘zgarishlar (ya’ni o‘lchovni o‘zgartirish, siljitish, aylanish), rasmni kesish, pikselni qayta joylash va hk kiradi
3. ***RSB***dan ***foydalanish protokoliga qarshi hujumlar,*** asosan, soxta RSBlarni, noto‘g‘ri stegolarni, RSB inversiyasini yaratish, bir necha RSBlarni qo‘shish bilan bog‘liq.
4. ***RSBning o‘ziga qarshi hujumlar*** - iloji bo‘lsa konteynerni buzmasdan, RSBni stegoxabaridan baholash va chiqarish. Bu guruhga kelishilgan hujumlar, statistik o‘rtacha hisobotlar, signallarni shovqindan tozalash usullari, ba’zi bir chiziqchiz filtrlash turlari va boshqalar kiradi.

Ushbu tasnifga muvofiq, RSBni joylashtirish tizimiga qo‘yiladigan barcha hujumlar to‘rt guruhga bo‘linadi:

– RSBni olib tashlashga qaratilgan hujumlar;
– konteynerni buzishga qaratilgan geometrik hujumlar;
– kriptografik hujumlar;
– joylashtirish va tasdiqlash uchun foydalanilgan protokolga qarshi hujumlar.

RSBni olib tashlashga qaratilgan hujumlar. Bu guruhda konteyner signallarini shovqindan tozalash, qayta modullash, yo‘qotishlar bilan siqish (kvantlash), o‘rtachalashtirish va kolliziya kabi hujumlar mavjud. Bu hujumlar RSB statistika sifatida tasvirlangan shovqin ekanligini taxminiga asoslanadi. Shovqinni yo‘q qilish maksimal ehtimollik yoki maksimal posteriorlik ehtimollari mezonlari yordamida signalni filtrlashni o‘z ichiga oladi. Shovqinni tozalash maksimal ehtimollik yoki maksimal posteriorlik ehtimollari mezonlarini qo‘llab shovqinni filtrlashdan iborat. Maksimal ehtimollik mezonini tatbiq qiluvchi filtr sifatida, StirMark dasturiy paketida ishlatiladigan median (RSB uchun Laplac tarqatish bilan) yoki o‘rtacha (Gauss taqsimoti uchun) filtrdan foydalanish mumkin.

Yo‘qotish bilan siqish va signalni shovqindan tozalash stegokanalning o‘tkazuvchanligini, yuzasi silliq tasvirlar uchun sezilarli darajada kamaytiradi. Bunday suratlarning o‘zgarish koeffitsenti suratni qayta tiklashga katta ta’sir qilmay “nollanishi” mumkin.

Qayta modulyatsiya- RSBga qarshi hujumlarga xos bo‘lgan nisbatan yangi usul. Hozirgi kunda steganosistemada ishlatiladigan dekoderga moslangan turli xil variantlari ma’lum. Hujumning tashkillanishida steganosistemaning barcha detallari ahamiyatga ega: $M-$ shaklli modulyatsiya, korellotsion decoder, shovqinga chidamli kodlarni qo‘llovchi steganosistemalar. Har qanday holda, RSB kengchiziqli signallar yordamida tasvirga o‘rnatilgan va butun tasvir ustida tarqaldi deb hisoblanadi. Dekoder tomonidan baholangan RSB haqiqiy bilan bog‘liq bo‘lgani sababli, dekoderni aldash mumkin. Hujum quyidagicha shakllantiriladi. Dastlab, himoyalangan tasvirdan tasvirning filtrlangan versiyasi chiqarilib, RSB "taxmin qilinadi". "Tahmin qilingan" RSB yuqori chastotali filtr ta’siriga tutiladi, qisqartiriladi, ikkiga ko‘paytiriladi va asl tasvirdan chiqarildi. Bundan tashqari, agar RSB kiritilganda, u joylashuvning ko‘rinmasligini oshirish uchun qandaydir niqobga ko‘paytirilgani ma’lum bo‘lsa,

tajovuzkor bu niqobni hisoblaydi va unga RSB ni ko‘paytiradi. Dekoderni “aldash” uchun qo‘shimcha chora sifatida yuqori chastotali hududlarda Gauss bo‘lmagan taqsimlash modellarini joylashtirish samara beradi. Shunday qilib, lineaviy korellatsion dekoderning optimalligi buziladi.

Bunday hujum faqat yuqori chastotali raqamli RSBlarga nisbatan samarali bo‘ladi, shuning uchun RSBning haqiqiy spektrlari asl tasvirning spektriga mos kelishi uchun quriladi. Gap shundaki, ishonchli baho faqat RSB ning yuqori chastotali komponentlari uchun olinadi. Hisobdan chiqarilishdan so‘ng, RSB ning past chastotali komponenti o‘zgarishsiz qoladi va detektorda ijobiy korrelyatsion javob beradi. Yuqori chastotali komponent esa nolga teng bo‘lgan salbiy javob berishi mumkin, va RSB aniqlanmaydi. Ushbu hujumga qarshi chora sifatida dastlab past-o‘tkazuvchi filtrlashni amalga oshirish taklif etildi.

RSBga qarshi yana bir samarali hujumga ***mozaika*** deyiladi. Ushbu hujum noqonuniy ravishda tarqalgan tasvirlarni kuzatadigan qidiruv tizimlariga qaratilgan. Rasm bir necha qismga bo‘linadi, shuning uchun qidirish mexanizmi RSBni aniqlamaydi. Internet-brauzer aslida bir-biriga yaqin bo‘lgan tasvirning bir nechta bo‘lagini ko‘rsatib turadi, bunda tasvir butunlay buzilmaydi. Ushbu turdagi hujumga qarshi kurashish uchun, tasvirning kichik qismlarida ham RSB aniqlanishi kerak. Bu tasvirning chekkalarini kesish uchun mustahkamlikdan ko‘ra murakkabroq, chunki oxirgi holatda buzg‘unchida tasvir sifatini saqlab qolish zarurati cheklangan. Ehtimol, rasmni "yig‘ish" va " RSB" ning mavjudligini tekshiradigan aqlli qidiruv tizimlarini yaratish maqsadga muvofiqdir.

Geometrik hujum. Olib tashlash hujumlaridan farqli o‘laroq, geometrik hujumlar RSBni olib tashlashga emas, balki ularni makon yoki zamon o‘zgartirishini kiritib o‘zgartirishni nazarda tutadi. Geometrik hujumlar dekoderga noma’lum parametrga ega afinniy o‘zgarishlar sifatida matematik tarzda modellashtirilgan. Jami beshta afinniy o‘zgarishlar mavjud: masshtabblash, proporsiyalarni buzish, burish, siljish va kesish. Ushbu hujumlar RSB detektorida sinxronlanishning yo‘qolishiga olib keladi va mahalliy yoki global bo‘lishi mumkin. Shu bilan birga, individual piksellarni yoki chiziqlarni kesish, ularning joylarini almashtirish, ba’zi o‘zgarishlarni qo‘llash mumkin. Bunday hujumlar Unsign (mahalliy hujum) va Stirmark (mahalliy va global hujum) dasturlarida amalga oshiriladi.

RSBlarni sinxronlash uchun ishlatiladigan nisbatan "aqlliroq" hujum usullari mavjud. Ushbu hujumlarning asosiy g‘oyasi, sinxronlash usulini va uni RSB amplitudasi spektrida tepaliklarni yumshatib yo‘q qilishdir. Hujumlar sinxronizatsiya qilish mexanizmi sifatida davriy shablon qo‘llanilgani sababli muvaffaqiyatlidir deb taxmin qilish mumkin. Bunday holda, sinxronizatsiyani ta’minlash uchun ikkita yondashuv qo‘llanilishi mumkin: tepaliklarning spektral hududga joylanishi yoki RSB ketma-ketligining davriy kiritilishi. Ikkala holatda ham tepaliklar spektrda shakllantiriladi, ular ko‘rib chiqilayotgan hujumda yo‘q qilinadi. Yo‘q qilinishdan so‘ng, boshqa geometrik hujumlardan foydalanish mumkin: sinxronizatsiya endi yo‘q.

Kriptografik hujumlar. Kriptografik hujumlar kriptografiya bo‘yicha analogga ega bo‘lgani sababli shunday nomlanadi. Ularga Orakul yordamida hujumlar, shuningdek, "qo‘pol kuch" yordamidagi hujum qilish kiradi.

Orakul hujumi, agar buyg‘unchi datchikga ega bo‘lsa, xavfsiz bo‘lmagan RSB tasvirini yaratishga imkon beradi. Usul detektorning qaysi tasvirga javob reaksiyasini ko‘rsatishi, qaysilariga ko‘rsatmasligini aniqlash maqsadida tajriba tadqiqotini o‘z ichiga oladi. Misol uchun, agar detektor "yumshoq" yechimlarni qabul qilsa, ya’ni signalda stego ehtimoli borligini ko‘rsatsa, shunda buzg‘unchi tasvirdagi kichik o‘zgarishlar detektorning xatti-harakatiga qanday ta’sir qilishini bilib olishi mumkin. Pikselli tasvirning har bir piksellini o‘zgartirib, detektor qaysi algoritmdan foydalanayotganini ham ko‘ra olish mumkin. "Qattiq" yechimli detektorda hujum chegara yaqinida amalga oshiriladi, bu yerda detektor o‘z yechimini "mavjud" dan "yo‘q" ga o‘zgartiradi.

Qattiq qarorli detektorga qilingan hujumga misol:

1. Stego xabarini o‘z ichiga olgan mavjud tasvirga asoslangan holda sinov surati yaratiladi. Tajriba tasviri turli xil usullarda yaratilishi mumkin, u detektor RSB yo‘qligini aniqlay olmaguncha original tasvirni o‘zgartiradi. Misol uchun tasvirni kontrastini asta-sekin kamaytirish, yoki har bir pikselni o‘zgartirib haqiqiy qiymatlarni boshqa biriga almashtirish mumkin.
2. Detektor RSBni aniqlamaguncha, tajovuzkor pikselning qiymatini oshiradi yoki kamaytiradi. Shunday qilib, bu RSB pixelning qiymatini oshirgani yoki kamaytirgani aniqlanadi.
3. 2-qadam tasvirdagi har piksel uchun takrorlanadi.

4. Detektorning har bir pikselning modifikatsiyasiga qanchalik ta’sirchanligini bilgan holda buzg‘unchi piksel tasvirni o‘zgartiradi, bu modifikatsiya tasvirni sezilarli darajada yomonlashishiga olib kelmaydi, ammo detektorning ishlashini buzadi.
5. Ushbu piksellar asl tasvirdan chiqariladi.

Foydalaniladigan protokolga qarshi hujumlar. Ko‘plab RSB steganosistemalari invers deb nomlanuvchi hujumlarga ayniqsa sezgridir. Ushbu hujum quyidagichadir. Buyg‘unchi himoyalangan tasvirdagi ma’lumotlarning bir qismi uning suv belgisiga egaligini aytadi. Shundan so‘ng, ushbu ma’lumot qismini chiqarib, qalbaki asl nusxani hosil qiladi. Qalbaki nusxada aslida haqiqiy RSB qismi bor. Boshqa tomondan, himoyalangan rasmda buzg‘unchi tomonidan e’lon qilingan yolg‘on RSB bor. Hal qilish murakkab vaziyat yuzaga keladi. Albatta, agar detektor asl tasvirga ega bo‘lsa, u holda identifikatorni aniqlash mumkin. RSB foydalanish protokoliga yana bir hujum turiga nusxalash hujumi kiradi. Ushbu hujum RSBni himoyalangan tasvirda baholash va baholangan boshqa RSB ni tasvirlarga joylashtirishdan iborat. Bundan maqsad, masalan, taqlid himoyasi yoki autentifikatsiya tizimiga qarshi turish mumkin.

Steganografik dasturlar bo‘yicha qisqa ma’lumot

Windows operatsion muhiti:

- **Steganos for Win** - fayllarni shifrlash va BMP, DIB, VOC, WAV, ASCII, HTML-fayllarda ularni yashirish uchun foydalanishi oson, xuddi shu vaqtda kuchli dastur. Foydalanish qulayligini yaratish uchun dastur usta sifatida yaratilgan. Ushbu 32-bitli dastur o‘zining qattiq diskdan fayllarni o‘chirib tashlaydigan Shredder ni o‘z ichiga oladi. Windows uchun Steganos yangi xususiyatlar va qo‘shimcha funksiyalar bilan fayllarni yashirish uchun axborot xavfsizligi bozorida jiddiy raqib hisoblanadi.
- **Contraband** BMP formatidagi 24 bitlik grafik fayllarni yashirish imkonini beruvchi dasturdir.

DOS operatsion muhiti:

- **Jsteg** - dastur mashhur JPG formatidagi ma’lumotlarni yashirish uchun mo‘ljallangan.
- **FFEncode** - matn fayliga ma’lumotlarni yashiradigan qiziqarli dastur. Dastur buyruq satridan tegishli parametrlardan boshlanadi.

- **StegoDos** - tasvirni tanlash, xabarni yashirish, ko‘rsatish va tasvirni boshqa grafik formatda saqlash imkonini beruvchi dasturiy paket.
- **Wnstorm** xabarni shifrlash va PCX formatidagi grafik fayl ichida yashirish imkonini beruvchi dasturiy paket.

OS/2 operatsion muhiti

- **Hide4PGP v1.1** - dastur BMP, WAV va VOC formatidagi fayllarni yashirish imkonini beradi va uni yashirish uchun har qanday sondagi kichik bitlardan foydalanish mumkin.
- **Texto** - Ma’lumotni ingliz tilidagi matnga aylantirgan steganografik dastur. Konvertatsiya qilinganidan keyin matnli fayllar-konteynerlar hech qanday mazmunga ega emas, lekin oddiy tekshirishdan o‘tish uchun yetarli darajada oddiy matnga o‘xshaydi.
- **Wnstorm** - DOS dasturiga o‘xshash.

Macintosh SHK uchun:

- **Stego** - PICT faylining ko‘rinishini va hajmini o‘zgartirmasdan ma’lumotlarni PICT formatidagi fayllarga joylashtirish imkonini beradi.
- **Paranoid** - bu dastur IDEA va DES algoritmlari yordamida ma’lumotlarni shifrlash va keyin faylni audio formatidagi faylda yashirish imkonini beradi.

Asosiy xulosalar

Insidentlar, virus infeksiyalarini tadqiq qilishning asosiy maqsadi hujumning oqibatlarini, uning kelib chiqish sabablari va usullarini aniqlashdan iborat. Hujumning sabablari va usullarini aniqlash orqali keyingi hujumlar va infeksiyalarning oldini olish uchun chora-tadbir ko‘rish mumkin.

Axborot xavfsizligi insidentlarini tekshirish jarayoni quyidagi bosqichlardan iborat: baholash, yig‘ish, tahlil qilish va hisobot.

Insidentlarning tergov bosqichida asosiy rolni: insident jurnallarini saqlash, foydalanuvchi vakolatlarini aniq ajratish, amalga oshgan xatti-harakatlar uchun mas’ul - bu hodisada ishtirok etgan shaxslarning dalillari va amalga oshirilgan harakatlar muhim ahamiyatga ega.

Insident haqida asosiy axborot manbalari: Helpdesk, foydalanuvchidan bevosita xabar, axborot xavfsizligi xodimlari aniqlagan insidentlar, jurnallar va ogohlantirish tizimlari.

Insidentlarni boshqarishda asosiy qiyinchiliklar quyidagi holatlardan kelib chiqadi: hodisani aniqlash va qayd qilish, hodisaning sabablari va oqibatlarini bartaraf etish, hodisani tekshirish, tuzatuvchi va profilaktik harakatlar amalga oshirilishi.

Insidentni tadqiq qilish, uning yuzaga kelishi uchun mas'ul shaxslarni aniqlash, hodisaning dalillari va dalillarini to'plash, tegishli intizomiy harakatlarning ta'rifini o'z ichiga oladi.

Hodisa va hozirgi vaziyat o'xshashliklarni topish zarur bo'lgan narsalar kabi ko'rinadi va bu holat uchun mavjud bo'lgan faktlarni uzatish orqali ushbu insidentga doir bir nechta xulosa chiqarish mumkin.

Steganografiya aloqaning mavjudligini aslida yashiradigan aloqa vositasi. Raqib yuborilgan xabarning shifrlangan matnni aniq-ravshan belgilashi mumkin bo'lgan kriptografiyadan farqli o'laroq, steganografik usullar maxfiy xabarlarni zararsiz xabarlarga kiritishga imkon beradi, shunda yashirin maxfiy xabarning borligiga shubha qilinmaydi.

Raqamli steganografiya - raqamli obyektlarga qo'shimcha ma'lumotni yashirish yoki kiritishga asoslangan, shu bilan birga ushbu obyektlarning bir qismida buzilishlarga olib keluvchi klassik steganografiyaning yo'nalishi.

Kompyuterning steganografik tekshiruvi turli xil fayllar, dasturlar, protokol paketlari va boshqalar bo'lgan kompyuter ma'lumotlarida axborotlarni yashirish usullarini o'rganadi.

Kompyuter steganografiyaning asosiy yo'nalishi audio va vizual ma'lumotlar ortiqchaligidan foydalanish hisoblanadi.

Steganografik tizim yoki steganosistema axborotni uzatish uchun maxfiy kanal yaratish maqsadida ishlatiladigan vositalar va usullar to'plami.

Steganosistemaga qarshi hujum kategoriyalari: joylangan xabarlarga qarshi hujumlar, stegodetektorga qarshi hujum, raqamli suv belgilari (RSB) dan foydalanish protokollariga qarshi hujum, RSB ning o'ziga qarshi hujum.

Nazorat uchun savollar

1. *"Insident" tushunchasi mohiyatini oching.*
2. *Axborot xavfsizligi insidentlarini tekshirish jarayoni.*
3. *Insident sodir bo'lganligi haqida asosiy ma'lumot manbalarini tushuntiring.*
4. *Nimalar insidentlar boshqarishda katta qiyinchiliklarga sabab bo'ladi?*

5. *Insidentni tekshirishning asosiy bosqichlarini tushuntiring.*
6. *Xavfsizlik insidentlarining toifalari qanday?*
7. *Kompyuter insidentlarini tekshirish elementlarining ro‘yxatini keltiring.*
8. *Axborot xavfsizligi insidentlarini hodisa tahlili uchun asos nima?*
9. *Hodisa tahlil qilish algoritmi modelini tushuntiring.*
10. *Steganografiya nimani anglatadi?*
11. *Steganografik yo‘nalish qanday tasniflanadi?*
12. *Steganografik tizimga hujumlarning asosiy turlari qanday?*
13. *Steganografik dasturlarning namunalarini keltiring.*

5. KOMPYUTER VOSITALARI VA TIZIMLARINI KRIMINALISTIK TADQIQ QILISH

5.1. Kriminalistik tadqiq

Kompyuter jinoyatlari jinoyat usullari va ularni sodir etgan shaxslar, jabrlangan taraflar va ushbu jinoyatlarga koʻmaklashadigan yoki oldini oladigan holatlar toʻgʻrisidagi umumiy kriminalistik xarakteristikasiga ega.

Kriminalistik texnika yoʻnalishi quyidagi meʼzonlarga javob bersa, shakllangan deb hisoblanadi:

– inson faoliyatining boshqa jabhalarida bunday obyektlarni oʻrganishda qoʻyilmaydigan aniq masalalarning kriminalistik yechimlari;

– tadqiqotning dalil obyektlarini xususiyatlari va, ayni paytda, ularning tarqalganligi, jinoiy va fuqarolik jarayonida tez-tez paydo boʻlishi;

– ushbu yoʻnalishni metodologik va metodik rivojlantirilganligi.

Kompyuter vositalari va tizimlarini **kriminalistik tadqiq qilish** statsionar kompyuterlar, serverlar, maʼlumot tashuvchilar hamda uyali aloqa vositalari, smartfonlar, planshet kompyuterlari va hokazolarning oʻrganilishini oʻz ichiga oladi.

Odatda, kompyuter vositalari va tizimlari ish materiallariga moddiy dalil sifatida qoʻshiladi, ammo ushbu qurilmalar xotirasida saqlanadigan maʼlumot kriminalistik tadqiq qilishning asosiy obyekti hisoblanadi. Maʼlumotlar bevosita shaklda taqdim etiladi va uni qabul qilish imkoniyatini taʼminlash uchun maxsus vositalardan foydalanish kerak.

Kriminalistik tadqiq qilishni oʻtkazish axborot xavfsizligi Insidentini tekshirishning muhim qismidir. Buning sababi axborot tashuvchilarida sodir boʻlgan hodisani yoritib berishi mumkin boʻlgan axborotni oʻz ichiga oladi va shuningdek, unga topshirilayotgan shaxslarni aniqlashga yordam beradi. Olingan maʼlumotlarga koʻra, kriminalistik tadqiq qilishning xulosasi dalil sifatida ishlatilishi mumkin.

Kompyuter axborotlari va kompyuter texnikasi boʻyicha kriminalistik tadqiq qilish quyidagi ishlarga asoslangan:

– axborot tizimidagi har qanday hodisalarning xronologiyasini tiklash;

– taxminiy ruxsatsiz kirish izlarini izlash;

– xatlarni qabul qilish va tahlil qilish (elektron pochta, lahzali xabar almashish dasturlari);

– mobil qurilmalarni kriminalistik tadqiq qilish;

– ma’lumotlar omborini tadqiq qilish;

– tarmoq trafigi damplarini, tezkor xotirani tadqiq qilish;

– kompyuterda mavjud bo‘lgan zararli dasturlarni qidirish;

– dasturiy mahsulotlarni plagiat mavjudligiga tekshirish;

– ularni olib qo‘yilgandan so‘ng kompyuter ma’lumotlarni saqlash vositalari tarkibining yaxlitligini (o‘zgarmasligini) o‘rnatish.

Kriminalistik ekspertizaning asosiy prinsiplari.

Kompyuter vosita va tizimlarini musodara qilish bilan bog‘liq tadqiq qilish o‘tkazish paytida, quyidagilarga amal qilish kerak:

– qo‘lga kiritilgan kompyuterlardagi axborotni o‘zgartirmaslik;

– sud ekspertizasini o‘tkazishning ilojisi bo‘lmagan holdagina ma’lumotga o‘sha joyning o‘zida kirish va tadqiq qilish mumkin;

– kompyuter va tizimlar bilan har qanday manipulyatsiya faqat mutaxassis ishtirokida amalga oshiriladi;

– bu harakatlar natijalari isbot sifatida foydalanishini ta’minlash maqsadida batafsil dalolatnoma orqali qayd qilinishi lozim.

Kompyuter vosita va tizimlarining kriminalistik tadqiq qilishga tadqiq qilishning zamonaviy imkoniyatlari kiritilishi lozim. Bu belgilangan obyektlarni o‘rganish davomida sud ekspertizasining asosiy yo‘nalishlari bo‘yicha tayinlangan masalalar bo‘yicha ko‘rsatiladi. Birinchi navbatda, bu sud kompyuter-texnika ekspertizasi sinfiga taaluqli. Unga quyidagilar kiradi:

– sud apparat-kompyuter ekspertizasi - kompyuter tizimi (moddiy ma’lumot tashuvchi) ning apparat vositalarini tadqiq qilish;

– sud dasturiy-kompyuter ekspertizasi - kompyuter tizimining dasturiy ta’minotini tadqiq qilish;

– (ma’lumotlarning) sud axborot-kompyuter ekspertizasi-foydalanuvchi yoki kompyuter tizimida axborot jarayonlarini tashkil etish uchun (belgilangan) dasturlar tomonidan tayyorlangan axborotni izlash, aniqlash, tahlil qilish va baholash;

– sud kompyuter-tarmoq ekspertizasi - uning vazifasiga ko‘rib chiqilgan ekspertiza turlarining deyarli barcha masalalari kiradi, ya’ni ish bo‘yicha fakt va vaziyatni aniqlashning apparat, dasturiy va informatsion aspektlarini hal qilish kiradi. Uning obyektlari ekspertiza turlaridan (apparat, dasturiy, informatsion) olingan bo‘lib, farq shundaki, ularning bari ma’lum tarmoq texnologiyasida faoliyat ko‘rsatadi.

Quyidagi ***umumilmiy tadqiqot usullari*** raqamli kriminalistikasida cheklanmagan holda ishlatiladi:

1. Kuzatish.
2. Baholash.
3. Tavsiflash.
4. Solishtirish.
5. Tajriba.
6. Modellashtirish.
7. Izoh.
8. Tahlil va sintez.
9. Bashorat.

Tasavvur qilaylik, jinoyat sodir etilgan joyda - poyabzal izi topilgan. Tadqiq qiluvchilar bu izni dalolatnomada qayd etadilar, keyin esa ular poyabzalning izini ko‘rganini aytishga tayyordirlar va sudya ular aslida nimani ko‘rganliklari to‘g‘risida shubha qilmaydi.

Kompyuter ma’lumoti esa butunlay boshqacha. Tasavvur qilaylik, "Insident joyida", ya’ni server diskidagi log-fayldagi yozuv topildi. Inson his qilish organlari uni idrok eta olmaydi. Ushbu yozuvni ko‘rish uchun quyidagi texnik vositalarning vositachiligiga muhtojmiz:

– qattiq disk (HDD) mexanizmi;
– ichki mikrodastur bilan HDD nazoratchisi (firmware);
– BIOS dasturiy ta’minoti va fayl tizimi (drayver);
– faylni ko‘rish uchun dasturiy ta’minot (masalan, "less" vyuveri);
– ekran drayveri;
– o‘z mikrodasturi bilan ta’minlangan apparat vositalari (klaviatura, monitor).

Umumilmiy bilan bir qatorda forenzikada aynan unga taalluqli ***maxsus tadqiq usullari*** ham qo‘llaniladi:

1. Maxsus kriminalistik axborot tizimlarini yaratish va qo‘llash.

2. Ommaviy ("Google" kabi), shuningdek, maxsus ("Eshelon" kabi) qidiruv tizimlaridan dalillarni aniqlash yoki tekshirish uchun foydalanish.

3. Asl foydalanuvchi yoki o‘zgartirilgan ma’lumotni o‘z ichiga olgan fayllardan ajratish uchun ma’lum fayllarning xesh-funksiyalarini yig‘ish.

4. Kelajakda sodir bo‘lishi ehtimoli mavjud Insidentlarni tadqiq qilish maqsadida ommaviy axborot vositalarining to‘liq tarkibini arxivlash.

5. Laboratoriya sharoitida shubhali dasturlarning xatti-harakatlarini o‘rganish uchun tarmoq xizmatlarini taqsimlash.

Jinoyatchilikka qarshi kurashda kompyuter kriminalistikasining **umumilmiy va maxsus usullari** quyidagi shakllarda qo‘llanilishi kerak:

1. Kompyuter texnik ekspertizasini ishlab chiqarish. AT-mutaxassislari boshqa turdagi ekspertizada ishtirok etishlari kerak. Misol uchun, dasturiy ta’minot ekzemplyaridan foydalanish huquqi narxini aniqlash bo‘yicha tovar (iqtisodiy) ekspertizani o‘tkazish. Mualliflik huquqining buzilishini isbotlash uchun bunday tajriba mutlaqo zarur. Odatdagi iqtisodchi bu sohada mavjud amaliyot bilan narx-navo dasturiy mahsulotlarining xususiyatlari bilan tanish emas.

2. Mutaxassislarning kompyuter ma’lumotlariga tegishli - taftish, olib qo‘yish, tekshirish va h.k. tadqiq qilish harakatlarini bajarishda ishtirok etish. Misol uchun, olib qo‘yilishi kerak bo‘lgan kompyuterni o‘chirib qo‘yish kabi oddiy vazifa. O‘chirishning hech qanday qiyin usuli yo‘q. Uni to‘g‘ri o‘chirish uchun ishning holatini tahlil qilish, har xil hodisalarning ehtimolligini ko‘rib chiqish va faqat shunga asosan o‘chirish usulini tanlash kerak.

3. Sud majlisida mutaxassisning ishtiroki. Sud zalidagi mutaxassis tarjimon kabi ish yuritishi, jarayonning ishtirokchilariga atamalarning ma’nolarini tushuntirib berishi, ma’lum texnik tafsilotlarning mazmunini aniqlashtirib berishi mumkin.

4. Tezkor xodimlarni va tadqiq qilishchilarni texnik vositalar bilan ta’minlash, ulardan mutaxassislar ishtirokisiz o‘z ishlarida mustaqil ravishda foydalanishlari mumkin.

5. Foydalanuvchilar va texnik mutaxassislarni raqamli dalillarni birlamchi joylashtirish usullari, ularni yo‘q qilishdan himoya qilish bo‘yicha o‘qitish. Kompyuter jinoyatlarining muhim qismi faqatgina tajovuzkorning maqsadi bo‘lgan axborot tizimining operatori jurnallarni, elektron xabarlarni, ishlatiladigan dasturlarni va boshqa potensial

dalillarni saqlashga e’tibor bermasligi sababli hal etilmagan. Yoki kelajakda bunday dalillar haqiqiy bo‘lishi uchun ularni qanday qilib saqlash kerakligini bilmasligi, yoki hatto raqamli izlarning borligidan shubha qilmasligi mumkin.

5.2. Ma’lumotni qayta tiklash

Raqamli axborot vositalari orqali muhim axborotni yo‘qotish va uning raqamli axborot vositalaridan foydalana olmasligi tasodif yoki buzilish, sifatsizlik, noto‘g‘ri foydalanish, hamda ma’lumotlar va jinoyatning “raqamli izlarini” yo‘q qilish maqsadida buzg‘unchining atayin harakati natijasi bo‘lishi mumkin.

Har xil saqlash vositalariga (qattiq disk, flesh-disklar va boshqalar) yozilgan ***o‘chirilgan yoki zararlangan ma’lumotlarni qayta tiklash*** quyidagilarni qayta tiklash yordamida amalga oshiriladi:

- har xil turdagi o‘chirilgan fayllar (hujjatlar, rasmlar, videofayllar va boshqalar);
- kompyuter viruslari ishidan keyingi ma’lumotlar;
- fayl tizimlarining mantiqiy shikastlanishidan keyingi ma’lumotlar;
- buzuq kompyuterdagi ma’lumotlarni saqlash vositalaridagi ma’lumotlar;
- dastur xatoligi tufayli zararlangan fayllar.

Kriminal ahamiyatli kompyuter ma’lumotlarini tashishi mumkin bo‘lgan obyektlar kategoriyalariga quyidagilarni kiritish mumkin:

- axborotni saqlash uchun qurilmalar;
- ma’lumotlarni kiritish/chiqarish qurilmalari;
- axborotni qayta ishlash qurilmalari;
- axborot kanallari orqali ma’lumotlarni uzatish qurilmalari;
- axborot tizimlari va komplekslari.

Kompyuter tizimlari va vositalarining o‘ziga xos xususiyatlari chet el amaliyotida raqamli dalillarning maxsus sinfining ajralishiga va u bilan ishlash metodlari va texnikasi tasvirlanishiga sabab bo‘ldi. Asl raqamli dalilni, uning dublikatini va nusxasini ajratib ko‘rsatish kerak. Original raqamli dalillar ushbu tashuvchilar bilan bog‘liq holda olib qo‘yilgan (qabul qilingan) vaqtidagi moddiy tashuvchidir va bunday axborot obyektlari hisoblanadi. Duplikat - asl moddiy muhitda saqlanuvchi barcha axborot obyektlarining to‘liq raqamli qayta ishlangan variantidir. Nusxa esa moddiy vositadan mustaqil ravishda axborot obyektlarida joylashgan ma’lumotlarning aniq ko‘rinishidir.

Agar kompyuter texnologiyalari bilan ishlash jarayonida shakllanadigan axborot materiallarini alohida guruhga aylantiradigan bo‘lsak, ularni "axborot texnologiyalari" deb atash maqbuldir, chunki ushbu izlarning shakllanishi axborot texnologiyalarini qo‘llashning o‘ziga xos xususiyatlaridan kelib chiqadi va ularni axborot texnologiyalari yordamida barcha uchun tushunarli shaklga keltirish mumkin. Kriminalistika nuqtai nazaridan bunday izlar qurollar, asboblar va mexanizmlar izlariga yaqin, chunki turli xil axborot texnologiyalari vosita sifatida ishlatiladi va muayyan foydalanuvchi harakatlarini bajarishda raqamli shaklda taqdim etilgan va saqlash vositasining xususiyatlarini va holatini o‘zgartirish orqali qayd etilgan ma’lumotlarning aniqligi ma’lum algoritm va qonuniyatlarga asosan shakllantiriladi.

Hozirgi vaqtda axborotni yozishning turli xil usullari va shunga muvofiq turli xil saqlash uskunalari va tashuvchi vositalari mavjud *:* qattiq magnit disklar, tezkor xotira, flesh xotira, optik va magneto-optik disklar.

Energiya bog‘liqligi prinsipiga ko‘ra, axborotni saqlash qurilmalari ikki turga bo‘lingan: energiyaga bog‘liq (tezkor xotira) va energiyaga bog‘liq bo‘lmagan (qattiq magnit disklar, flesh xotira, optik va magneto-optik disklar). Quvvat o‘chirilganda, energiyaga bog‘liq xotira o‘chiriladi, energiyaga bog‘liq bo‘lmagan xotiralar esa quvvat yopilganda ma’lumotni saqlaydi.

Axborotni saqlash uchun yozib oluvchi qurilmalar barqarorligiga ko‘ra, doimiy saqlash qurilmalariga (BIOS); yoziladigan (CD-R); ko‘p marta qayta yoziladigan (CD-RW, DVD-RW, qattiq magnit disklar, flesh xotira); operativ qurilmalarga bo‘linadi.

Saqlash uskunalari boshqa asoslarga ko‘ra tasniflanishi mumkin, ammo ular ushbu obyektlar bo‘yicha tadqiq qilishning o‘ziga xos xususiyatlarini va qo‘llanilgan texnik vositalarni aniqlaydi. Axborotni saqlash qurilmalarini olib tashlashda, birinchi navbatda, energiyaga bog‘liq bo‘lgan xotira ichidagi ma’lumotlarni olib tashlash va saqlash tartibini aniqlash muhim ahamiyatga ega.

Kirish qurilmalari kiruvchi buyruqlarni ishlash uchun qulay bo‘lgan formaga aylantirish uchun mo‘ljallangan. Ularga klaviaturalar, manipulyatorlar, sensorli ekranli planshetlar (mobil qurilmalar bilan adashtirmaslik), interfaol dosklar, skanerlar, veb-kameralar, video ta’qib qilish qurilmalari, audio kirishli ovozli kartalar, smart-kartani o‘qiydigan asboblar, akselerometrlar va girodkoplar, yo‘ldosh

navigatsion qurilmalari , papillar va ko‘z to‘r pardasi naqshlari skanerlari, har xil sensorlar va o‘lchov asboblari, shuningdek boshqa qurilmalar kiradi. Ma’lumotlarni kiritish qurilmalarining asosiy elementi - bu analog va raqamli konverter bo‘lib, vazifasi turli tabiatdagi (mexanik, elektr, akustik va boshqalar) signallarni ishlash uchun mavjud bo‘lgan raqamli shaklga aylantirishdir.

Axborotni chiqarish qurilmalari raqamli formadagi ma’lumotni o‘qiladigan shaklga aylantirish uchun mo‘ljallangan. Bunga indikatorlar, monitorlar, proektorlar, printerlar, ovozli kartalar, bajaruvchi mexanizlar va telemexanika (masalan, turniket yoki elektron qulf) kiradi.

Axborotni qayta ishlash moslamalari algortim asosida kiruvchi axborotlarni qayd etish va nazorat qilish komandalarini shakllantirish uchun mo‘ljallangan. Shaxsiy kompyuterning tarkibiy qismlari orasida axborotni qayta ishlash qurilmasi misoli markaziy protsessor, grafik tekshiruvchi (video karta), ovoz protsessoridir (ovoz kartasi). Axborotni qayta ishlash qurilmalari odatda tezkor xotirani o‘z ichiga oladi, ular qayta ishlangan ma’lumotlarni saqlash uchun foydalaniladi (kesh, bufer). Deyarli har bir raqamli qurilma u yoki bu shaklda ma’lumotni qayta ishlovchi qurilma- mikrokontrollerga ega. U ma’lumotni mikrodasturda joylashgan va doimiy yodda saqlash qurilmasida (BIOS) saqlanuvchi algortim bo‘yicha qayta ishlaydi.

Aloqa kanallari orqali ma’lumotni uzatish qurilmalari signallarni ishlab chiqarish, ularni uzatish va turli xil aloqa kanallari (simli va simsiz) orqali qabul qilish uchun mo‘ljallangan. O‘zlarining tabiatiga ko‘ra ular kiruvchi ma’lumotlarni aloqa kanali (modulyatsiya) orqali uzatish uchun mos signalga aylantiradigan va uni uzatish, shuningdek signallarni qabul qilish va ularni qayta ishlash uchun mavjud bo‘lgan shaklga o‘tkazish (demodullash) ga aylantiruvchi ma’lumotli kirish/chiqarish moslamalaridir. Ma’lumot uzatish qurilmalari orasida modemlar, bluetooth-modullari, Wi-Fi routerlari va adapterlar, tarmoq kartalari, GSM-modullari, kommutator, marshrutizatorlar va infraqizil aloqa modullari mavjud .

Zamonaviy kompyuter, uning qurilmaviy xususiyatlariga (server, noutbuk, smartfon yoki planshet bo‘ladimi) qaramasdan, ro‘yxatdagi qurilmalarning barcha turlarini o‘z ichiga oladi va aslida birlashgan axborot kompleksi hisoblanadi. Ushbu axborot kompleksini boshqarish va komponentlarning o‘zaro ta’siri dasturiy ta’minot orqali amalga oshiriladi. Ushbu axborot tizimlarini qo‘llashning asosiy vazifasi axborotni qayta ishlash va foydalanuvchi tomonidan talab qilinadigan

natijalarni shakllantirishdan iborat. Shunga koʻra, har qanday axborot kompleksi yoki tizimining uchta asosiy komponenti mavjud: apparat, dasturiy va axborot.

Muhim maʼlumotlarni uzatish va saqlash nafaqat statsionar kompyuter texnikasi va tizimlari , ularning mahalliy va global tarmoqlar bilan munosabati uchun, balki hozirda keng tarqalgan mobil, uyali telefonlar, smartfonlar, planshetli kompyuterlar tadqiq qilish uchun eng muhim obyektlardir, negaki ular kriminalistika jihatdan qimmatli maʼlumotni tashuvchi va tarqatuvchi vosita boʻlish bilan birga jinoyatni sodir etish quroli hamdir. Ushbu qurilmalar endi elektron kompyuter sifatida tasniflana olmaydi, chunki ular tarmoq bilan doimiy aloqada boʻlib, uning bir qismi boʻlib hisoblanadi. Ular shaxsiy kompyuter, aloqa moslamasi, kommutatsiya kabilarni oʻz ichiga olgan integratsion qurilmalardir; muayyan dasturiy taʼminotdan foydalanadi; axborot tashuvchilarini (SIM-kartalar, xotira kartalari, USB-xotiralar) oʻz ichiga oladi; foto va video kameralar bilan jihozlangan global manzilni aniqlash tizimining (GPS) funksiyalarini bajaradi.

Raqamli shaklda saqlanadigan maʼlumotlarning oʻziga xos xususiyatlari quyidagicha:

– aniq boʻlmagan shakl, taqdim etish uchun maxsus vositalardan foydalanishga ehtiyoj;

– eng qisqa vaqt ichida va masofadan turib yoʻq qilish yoki oʻzgartirish imkoniyati;

– ushbu axborotdan foydalanishni cheklovchi maxsus vositalar mavjudligi;

– foydalanuvchi va turli operatsiyalar davomida doimiy axborot oʻzgarishi;

– aloqa kanallari orqali maʼlumotlarni uzatishda bir vaqtning oʻzida turli xil qurilmalarda oʻzaro bogʻliq axborotni shakllantirish.

Raqamli maʼlumotlarni roʻyxatga olish xususiyatlari raqamli dalillarni aniqlash va olishda, shuningdek, ularning sud-ekspertizasida maʼlum qoidalarga rioya qilishni talab qiladi.

5.3. Kompyuter texnik ekspertiza

Zamonaviy axborot texnologiyalari sohasidagi maxsus bilimlarni jalb qilmasdan, kompyuterdan ushbu jinoyatni tayyorlash, amalga oshirish yoki yashirish uchun foydalanilganda kompyuter

ma’lumotlariga ruxsatsiz kirishni o‘rganish va taftish etish mumkin emas.

Kompyuter texnologiyalari yordamida sodir etilgan jinoyatlar ushbu sohada maxsus bilimlarga ega bo‘lgan mutaxassislarsiz to‘liq va obyektiv tekshirilishi mumkin emas. Kompyuter texnologiyalaridan foydalanish bilan sodir hollarda maxsus bilimdan foydalanishning asosiy protsessual shakli kompyuter-texnik ekspertiza hisoblanadi.

Buning sababi shundaki, faqat mutaxassisning tahlili apparat vositalari, dasturiy ta’minot va kompyuter ma’lumotlarini o‘rganishda katta ahamiyatga ega.

Aynan mutaxassis izlanishi qo‘lga kiritilgan apparat, dasturiy ta’minot va kompyuter ma’lumotlariga dalil bo‘lish uchun qiymat beradi. Bunday hollarda tadqiq qilishchining asosiy vazifalari - zarur moddiy obyektlarini - axborot tashuvchilarni qidirish, aniqlash, olib tashlash va ularni topshirish hisoblanadi.

Kompyuter-texnik ekspertizasining quyidagi turlari mavjud:

- avtomatlashtirish vositalari (hisoblash tizimlari, ma’lumotlarni uzatish va nusxalash vositalari) yordamida tayyorlangan matnli va grafik hujjatlar (standart va elektron);
- ularning faoliyati uchun zarur bo‘lgan kompyuter dasturlari va yordamchi kompyuter ma’lumotlari;
- video va audio yozuvlar, multimedia formatida taqdim etilgan vizual va audio axborot;
- (ma’lumotlar bazalari) avtomatlashtirilgan saqlash, qidirish, ishlov berish va uzatishni ta’minlaydigan formatda taqdim etilgan kompyuter ma’lumotlari va hujjatlar;
- turli moddiy axborot tashuvchilar (magnit, magnit-optik, optik va boshqalar).

Shunga ko‘ra, kompyuter-texnik ekspertiza quyidagi vazifalarni hal qilishi mumkin deb aytiladi:

1. Moddiy axborot vositalarida mavjud bo‘lgan ma’lumotlarning to‘liq yoki qisman qayta takrorlanishi va nashr etilishi, shu jumladan matn bo‘lmagan shaklda.

2. Avvallari moddiy axborot vositalarida saqlangan va keyinchalik turli sabablarga ko‘ra o‘chirilgan yoki o‘zgartirilgan axborotni qayta tiklash.

3. Muayyan axborotni kiritish, o‘zgartirish, yo‘q qilish yoki nusxalash vaqtini belgilash.

4. Kodlangan ma’lumotlarning parolini bekor qilish, parollar tanlash va axborotni himoya qilish tizimini ochish.

5. Hujjatlarni (fayllarni, dasturlarni) ishlab chiqarish, tayyorlash, joylashtirish vositalarini yaratish.

6. Avtomatlashtirilgan axborot tizimlarining dasturiy-apparat komplekslarining texnik holatini, ularning sozligini, muayyan foydalanuvchi uchun moslashtirish imkoniyatini aniqlash.

Kompyuter vositalari (apparat, dasturiy, axborot) ni ta’minlash va uni har qanday kompyuter tizimlarini ishlab chiqish va ishlatish jarayoniga mos keladigan shaklda foydalanish asosida kompyuter texnik ekspertizasi turlarining tasniflanishini tashkil etish maqsadga muvofiq. Shuning uchun quyidagilarni ajratish mumkin: (ma’lumotlarni) **apparat-texnik va dasturiy-texnik ekspertiza**. Bundan tashqari tarmoq va telekommunikatsiya texnologiyalaridan foydalanish bilan bog‘liq faktlar va holatlarni o‘rganish uchun **kompyuter-tarmoq** ekspertizasini ajratish juda haqli ko‘rinadi.

Apparat-texnik ekspertizaning mohiyati texnik (apparat) kompyuter texnikasining vositalarini o‘rganishdir. Ekspertizaning maqsadi - kompyuter tizimi apparaturasi - kompyuter ma’lumotlariga ruxsatsiz kirish yoki haqiqat to‘g‘risida axborotni etkazib beradigan materiallarni etkazib beruvchilarning faoliyatiga tegishli qonunlarni o‘rganish asosida belgilangan faktlar va holatlardir.

Dasturiy-texnik ekspertizaning maqsadi bu funksional vazifasi, xususiyatlari va amalga oshirish talablarini, algoritm va kompyuter tarkibiy xususiyatlarini, taqdim etilgan tizim dasturiy ta’minotining hozirgi holatini o‘rganish hisoblanadi.

Kompyuter tarmoq ekspertizasi obyektlari internetga ulangan foydalanuvchilarning kompyuterlari va tarmoq provayderlari (Internet-provayderlar) ning turli xil resurslari, shuningdek ular tomonidan ko‘rsatiladigan axborot xizmatlari (elektron pochta, elektron xabarlar xizmati, yangiliklar guruhlari, WWW xizmatlari va boshqalar) bo‘lishi mumkin.

Apparat-texnik ekspertizasida mutaxassis oldiga quyidagi - quyidagi savollarni qo‘yish tavsiya etiladi:

1. Tadqiqotda qaysi kompyuter modeli namoyon bo‘ladi , atrof-muhit qurilmalarining parametrlari, kompyuter tarmog‘i gatexnik xususiyatlari qanday?

2. Kompyuter va uning komponentlari uchun texnik hujjatlar mavjudmi? Mavjud bo‘lganlar mos keladimi?

3. Kompyuterni va uning tarkibiy qismlarini yig‘ish uchun shart-sharoitlar qanday: markali yig‘ilish, boshqa kompaniyaning tarkibiy qismlaridan yig‘ish yoki qo‘l ishimi? Asosiy paketga kiritilmagan qo‘shimcha qurilmalar mavjudmi (asosiy paket hujjat bo‘yicha aniqlanadi)?

4. Ayrim jihozlar, magnitli saqlash vositalarining (turli test dasturlari tomonidan aniqlangan) kamchiliklari mavjudmi?

5. Kompyuter muayyan foydalanuvchilarga (chapaqay, ko‘zi ojizlar va boshqalar) moslashtirilganmi?

Dasturiy-texnik ekspertizaga quyidagi masalalar qo‘yiladi:

1. Kompyuterda ishlatiladigan operatsion tizimning turi nima?

2. Ushbu kompyuterda qaysi dasturiy mahsulotlar ishlatiladi? Ular litsenziyalanganmi, "pirat" nusxalarimi yoki ular aslmi? Dastur ma’lumotlari qachon o‘rnatilgan?

3. Dasturiy mahsulotlarni vazifasi nima? Ular qanday amaliy masalalarni hal qilish uchun mo‘ljallangan? Ma’lumotni kiritish va chiqarishning qanday usullari qo‘llaniladi? Dasturlarning ishlash natijalari kerakli harakatlarga mos keladimi?

4. Qaysi dasturiy ta’minotni himoya qilish usullari (parollar, identifikatsiyalash kodlari, xavfsizlik dasturlari va boshqalar) ishlatiladi? Ruxsatsiz kirish, parollarni aniqlash yoki boshqa urinishlar sodir etilganmi?

5. Yashirin fayllarda qanday ma’lumotlar mavjud? Avval o‘chirilgan fayllarni tiklash mumkinmi va uning mazmuni qanday bo‘ladi?

6. Anti-virus, fayllarning nazorat miqdorini tekshirish dasturlari natijalari qanday shaklda saqlanadi?

7. Ma’lum dasturlarda nosozliklar mavjudmi? Ushbu kamchiliklarning sabablari nima?

8. Magnit fayllardagi fayllar nimani o‘z ichiga oladi va uning holati qanday? Ushbu fayllar oxirgi marta qachon o‘zgartirilgan?

Tadqiqot amaliyotidan misol keltiramiz:

K... o‘zining kompyuteri orqali “Internet” tarmog‘iga ruxsatsiz kirishni amalga oshirgan. Bunda u “troyan oti” dasturiga o‘xshash zararli dastur yordamida nusxa olgan va qo‘lga kiritilgan login hamda parollardan foydalangan.

Ish bo‘yicha dasturiy ta’minot va texnik ekspertizani o‘tkazish tayinlangan. Ekspertga quyidagi savollar qo‘yilgan:

1. Tizim blokining ishlashi haqida taqdim etilgan qattiq diskda qanday dasturlar mavjud?

2. Ushbu tizimda Internetga kirish uchun ishlatiladigan dastur mavjudmi?

3. Masofadan kirish uchun belgilar tizim blokida mavjudmi?

4. Qaysi loginlar, parollar va kirish telefonlari (dialerlar) har bir belgiga mos keladi?

5. Kompyuter tarmoqlari va tizimlariga ruxsatsiz kirish uchun tizim blokining qattiq diskida dastur mavjudmi (skanerlash portlari, troyan otlari, keyloggerlar va h.k.)?

6. Elektron pochta va yangiliklar bilan ishlash uchun tizim birligida qanday dastur ishlatilgan?

7. Xabarlar qaysi elektron pochta manzilidan kelishi va qaysi e-pochta manzillariga yuborilganligi haqida ma’lumot bormi?

8. Qattiq diskda qanday pochta qayd yozuvlari mavjud?

9. E-pochtada zararli dasturlardan iborat fayllar mavjudmi?

10. Qabul qilingan xabarda Internetga kirish uchun parollar bormi?

Kompyuter-tarmoq ekspertiza davomida quyidagilar haqida savol berish zarur:

1. Kompyuter tarmog‘i faoliyati uchun qanday dastur ishlatiladi? Bu litsenziyalanganmi?

2. Kompyuterlar tarmoqqa qanday bog‘langan? Global kompyuter tarmoqlariga kirish imkoni bormi?

3. Qanday kompyuterlar tarmoqning serverlari hisoblanadi? Korxona, muassasa, tashkilot, firma yoki kompaniyada kompyuter tarmog‘ining tugunlarida axborot uzatish qanday amalga oshiriladi?

4. Axborotdan foydalanishni cheklash uchun kompyuter tarmog‘i parollari, identifikatsiya kodlari foydalanilganmi? Ular qanday shaklda ishlatiladi?

5. Alohida dasturlar va kompyuterlarning tarmoqning bir qismi sifatida ishlashida biron-bir nosozlik bormi? Ushbu kamchiliklarning sabablari nima?

6. Qaysi axborot kompyuter tarmog‘i orqali uzatiladi, qayta ishlanadi va o‘zgartiriladi?

Tadqiq qilishning muvaffaqiyatli natijasi ekspertning tekshiruv, qidiruv, olib qo‘yish va ma’lumotlarni kompyuter texnikasi yordamida o‘rganishidagi ishtirokiga bog‘liq.

Kompyuter-texnik ekspertiza bo‘yicha maxsus bilimlar elektronika, elektrotexnika, axborot tizimlari va jarayonlari, radiotexnika va kommunikatsiyalar, kompyuter texnologiyalari, jumladan, dasturlash va avtomatlashtirishdan iborat.

Ekspert xizmatlariga ehtiyoj. Texnika bugun ko‘p jihatdan inson mehnatini o‘rnini bosgan, axborotning katta miqdori endilikda axborot vositalarining turli xil tashuvchilarida saqlanadi. Shuning uchun, har qanday nizo yoki ish olib borishda kompyuter apparati va dasturiy ta’minot sohasidagi mutaxassis bilan maslahatlash ehtiyoji bor.

Jinoiy ishlarning daliliy asoslaridan tashqari, sud ishlarini yuritishning boshqa sohalarida ekspert tekshiruvi talab etiladi.

Sudgacha bo‘lgan bahs-munozaralarda, iste’molchining iltimosiga ko‘ra, kompyuter tizimlarining sifatini tekshirish natijalari (xizmat ko‘rsatish, ta’mirlash va boshqalar) taqdim etiladi. Qoida tariqasida, bu holatda, mutaxassisning asosiy vazifasi, ularning narxini aniqlash uchun uskunaning kamchiliklarini tahlil qilishdir. Bu yerda kompyuter va komponentlar bilan bog‘liq bo‘lgan har qanday muammolarning mavjudligi, ularning sifati o‘zgarishi, undan foydalanish imkoniyati masalalari va h.k. haqidagi umumiy xulosa talab etiladi. Bunday yo‘lda, nafaqat real vaziyat belgilanadi, balki zarar to‘lovlar (kompensatsiya) hajmi aniqlanadi.

Sud kompyuter-texnik ekspertizasi obyektlari.

Apparat obyektlari

- shaxsiy kompyuterlar (ish stoli uchun moslashgan, portativ);
- periferiya qurilmalari (printerlar, modemlar va h.k.);
- tarmoq uskunalari (serverlar, ishchi stansiyalari, faol uskunalar, tarmoq kAbellari va boshqalar);
- integratsiyalashgan tizimlar (tashkilotchilar, peyjerlar, mobil telefonlar va boshqalar);
- barcha komponentlarning to‘ldiruvchi vositalari (apparat bloklari, kengaytirish kartalari, xotira kartalari, magnit va lazerli disklar, magnit lentalar, kartalar va boshqalar).

Dastur obyektlari

- kompyuter tizimli dasturiy ta’minoti;

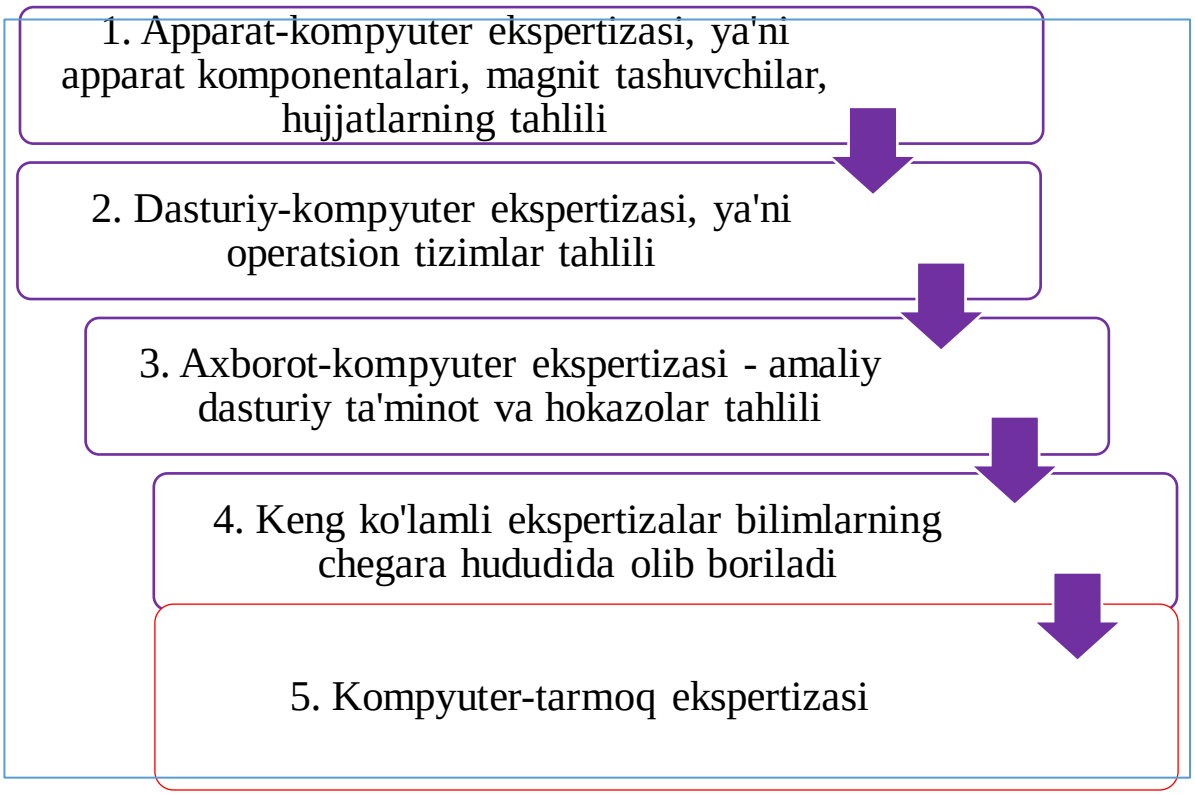
- kompyuter amaliy dasturiy ta’minoti.

Axborot obyektlari (ma’lumotlar)

- kompyuter vositalarini qo‘llab yaratilgan hujjatlar;
- kompyuter ma’lumotlarining multimediya formatida ma’lumotlar;
- ma’lumotlar bazasi va boshqa ilovalardagi to‘ldiruvchi xususiyatga ega kompyuterlashtirilgan ma’lumotlar.

1,2,3-ilovada raqamli kriminalistikada qo‘llaniluvchi apparat va dasturiy vositalar hamda ishlab chiqaruvchi to‘g‘risida ma’lumotlar keltirilgan.

Ekspertiza turlari (23- rasm):



23- rasm. Ekspertizalarning ketma-ketligi

1. Apparat-kompyuter ekspertizasi, ya’ni apparat komponentlari, magnit materiallar, hujjatlarni tadqiq qilish.
2. Dasturiy-kompyuter ekspertizasi, ya’ni OS tadqiqotlari.
3. Axborot-kompyuter ekspertizasi – amaliy dasturiy ta’minot va h.k tahlili.
4. Keng ko‘lamli ekspertizalar bilimlarning chegara hududida olib boriladi.

5. Kompyuter-tarmoq ekspertizasi.

Apparat-kompyuter ekspertizasi apparat uskunalari va kompyuter texnologiyasidan foydalanish qonuniyatlarini aniqlash va o‘rganishdir. Apparat-kompyuter ekspertizasi jarayonida apparat vositasining markasini, turini, xususiyatlarini, shuningdek, ularning barcha texnik xususiyatlarini aniqlash mumkin.

Ushbu turdagi ekspertiza kompyuterlarni o‘rganish, ya’ni qurilmaning namunasini, texnik ko‘rsatkichlarini, turini, modelini aniqlash uchun mo‘ljallangan. Shuningdek, apparat-kompyuter ekspertizasi yordamida tarmoq yoki tizimdagi muayyan kompyuter qurilmasining funksional maqsadlari va funksional parametrlarini, dastlabki texnik holatini va apparatning konfiguratsiyasini, shuningdek, o‘rganilayotgan vaqtdagi holat va konfiguratsiyani o‘rnatish mumkin.

Ushbu turdagi ekspertiza predmeti kompyuter tizimini-jinoyat ish amalga oshirilgani to‘g‘risidagi ma’lumotni tashuvchi moddiy vositalarni qo‘llash bo‘yicha tahlil asosida aniqlangan faktlar va vaziyatlardir.

Bugungi kunda sud apparat-kompyuter ekspertizasi quyidagi vazifalarni hal qiladi:

– ba’zi funksional vazifalarning yechimlarini uchun apparat vositasining turi xususiyatlari, texnik va funksional belgilarini aniqlash;

– vositaning hozirgi holati va ishlashi, nuqsonlar mavjudligi aniqlash;

– aniqlovchi apparatlardan yakka yoki kompyuter tizimi tarkibi sifatida kompleks qo‘llash orqali mexanizm strukturasini va hodisa vaziyatini uning natijasiga asoslanib aniqlash;

– apparat vositasining o‘ziga xos qobiliyatlaridan foydalanish natijasi va ulardan foydalanish o‘rtasidagi sababchi munosabatlarni o‘rnatish;

– apparat vositasidan qo‘llash shartlarini (tuzilishini) aniqlash, ulardan foydalanishning xronologik ketma-ketligini tiklash, ishlatish va ishlash joyini aniqlash.

Dasturiy-kompyuter ekspertiza kompyuterlar dasturiy ta’minotini o‘rganadi. Ushbu ekspertiza dasturiy ta’minotni quyidagicha tahlil etadi:

– dasturiy ta’minot va uning komponentlarining umumiy xususiyatlari;

– ishlab chiquvchilar va huquq egalarining tafsilotlari;

– ishlab chiqarilgan sana, dasturning hajmi;

– apparatga qo‘yiladigan talablar, dasturiy ta’minot qobig‘i va ma’lum bir kompyuterda boshqa dasturlar bilan dasturiy muvofiqligi, dasturning ishlashi;

– o‘rganilayotgan dastur o‘zgarmaganmi, o‘zgartirilgandan so‘ng olingan dasturning yangi xususiyatlari, vaqti, maqsadlari, o‘zgarish tarkibi;

– zararli dastur yo‘qmi, uning foydalanish oqibatlari qanday.

Jinoiy ishda haqiqatni aniqlash uchun tadqiqotga taqdim etilgan dasturiy ta’minotning kompyuter tizimini ishlab chiqish va ulardan foydalanish qonunlari predmet hisoblanadi.

Dasturiy ta’minot va kompyuter ekspertizasining hal etiluvchi vazifalari quyidagilardan iborat:

– mazkur kompyuter sistemasining tashuvchilaridagi dasturning asli va nusxasini aniqlash;

– umumiy belgilar asosida dasturiy ta’minotning guruhga tegishli ekanligini belgilash;

– mualliflikni aniqlashga olib keluvchi dasturning ma’lum belgilarini aniqlash;

– o‘rganilayotgan kompyuter muhiti bilan o‘zaro bog‘liqlikni aniqlshga olib keluvchi dasturning ma’lum belgilarini aniqlash;

– operatsion tizimning asosiy belgilarini aniqlash;

– dasturiy ta’minotning funksional xususiyatlarini, sozlamalarini, o‘rnatilish vaqtini (mashina tashuvchisiga o‘rnatilish) aniqlash va o‘rganish

– dastur obyektining holatini, unga tegishli fayllar tarkibini, ularning parametrlarini (hajm, yaratilish sanasi, qurollari), ma’lumotni kiritish/chiqarish usullarini, tur parametrlaridan farqlanishning mavjud yoki yo‘qligi;

– dastur mahsulotining (dastur mahsuloti, grafik yoki matnli fayl shaklidagi) algoritmini tashxis etish;

– dastur mahsulotini (algoritmi) ishlab chiqishda qo‘llanilgan qurol turlarini aniqlash;

– dastur mahsulotini qo‘llab-quvvatlovchi apparat-dastur platformalarining turlarini aniqlash;

– dasturning ilk holati (masalan, ilk o‘rnatilishdagi) va keyingi sodir bo‘lishi mumkin bo‘lgan o‘zgarishlarni (yangilanish, tarkib o‘zgarishi) belgilash;

– dasturiy ta’minotning holati va xususiyatlarini o‘zgartirishning maqsadi va shartlarini aniqlash (ma’lum funksiyalarning atayin o‘zgartirilishi, aniq bir apparat muhitiga konfiguratsiyalash);

– dasturda o‘zgartirishlarni amalga oshirish usullarini aniqlash (masalan, zararli dastur ta’siri, dastur muhitidagi nosozliklar, ruxsatsiz kirish)

– qayta ishlanayotgan ma’lumotlar (xizmat, tizim fayllari tarkibiga ko‘ra), ta’minlovchi apparat vositalariga asosan dasturning xususiyatlari va holatini aniqlash;

– dasturiy ta’minotning harakatdagi faoliyati natijasiga ko‘ra mexanizm strukturasini aniqlash;

– kompyuter tizimi foydalanuvchisining dasturiy ta’minotga nisbatan bajargan ishlari va oqibatlar o‘rtasidagi aloqani aniqlash.

Axborot-kompyuter ekspertizasi kompyuter-texnik ekspertizaning asosiy turi hisoblanadi. Bu axborotni kompyuterga oid diagnostika va identifikatsiyalash masalalari bilan yakuniy hal qilish orqali dalil bazasining ajralmas qismini to‘ldirishga imkon beruvchi tekshiruvdir. Ushbu turdagi ekspertizalar foydalanuvchi ma’lumotlari va dastur tomonidan yaratilgan axborotlarni tekshiradi.

Bunday ekspertiza maqsadi kompyuter axborot jarayonlarini tashkil etish uchun foydalanuvchi yoki dasturlar tomonidan hosil qilingan (yaratilgan) axborotni izlash, aniqlash, tahlil qilish va baholash hisoblanadi. Axborot -kompyuter ekspertizasi davomida quyidagilar aniqlanadi:

– tashuvchiga yozilgan qayd turlari;

– ma’lumotlarning jismoniy va mantiqiy joylashuvi;

– tashuvchidagi ma’lumotlarning xususiyatlari, belgilari, turi va parametrlari;

– ma’lumotlarning barcha uchun ochiqligi, himoya vositalarining mavjudligi, vositalardan o‘tish belgilarining borligi;

– axborot mazmuni, uning operatsiya ma’lumotlari bilan amalga oshirilgan ilk holati, amaliyot, ya’ni, nusxa ko‘chirish, o‘zgartirish, bloklash, yo‘q qilish, bu operatsiyalar xronologiyasi.

Oldingi tarmoqlardan farqli ravishda, **kompyuter-tarmoq ekspertizasi** asosan, ba’zi tarmoq axborot texnologiyasini amalga oshiradigan kompyuter vositalarining funksional maqsadlariga asoslanadi. Kompyuter tarmog‘i ekspertizasi predmeti tarmoq va

telekommunikatsiya texnologiyalaridan foydalanish bilan bog‘liq faktlar va sharoitlardir.

Kompyuter - tarmoq ekspertiza quyidagi vazifalarni hal qilish uchun o‘tkaziladi:

– apparat vositasi va dasturiy ta’minot xususiyatlari va belgilarini aniqlash, o‘rganilayotgan obyektning tarmoqdagi o‘rni, roli va funksional vazifasini aniqlash (masalan, dastur vositasi uchun- tarmoq operatsion tizimiga nisbatan; apparat vositasi uchun- server, ish stansiyasi, faol tarmoq moslamasiga nisbatan);

– hisoblash tizimi belgi va xususiyatlarini aniqlsh, uning arxitekturasi, konfiguratsiyasini belgilash, joylangan tarmoq komponentini aniqlash, ma’lumotlarga kirishni tashkillashtirish;

– vositaning ilovadagi server yoki mijoz qismiga tegishli ekanligi;

– tarmoq vositasining holati va sozligini, jismoniy nuqsonlar mavjudligini, tizim jurnalining holatini, kirishni nazorat qilish komponentlarini aniqlash;

– hisoblash tizimining umumiy va har bir tizim vositasi uchun alohida ilk holatini, xarid uchun joy, ilk konfiguratsiyaga kiritilgan o‘zgartirishlarni (masalan, qo‘shimcha tarmoq vositalarini, server yoki ish stansiyasiga kengaytma qurilmalarini kiritish) aniqlash;

– hisoblash tizimidagi o‘zgarishlar sababini aniqlash (masalan, foydalanish darajasini nazorat qilish bo‘yicha, tarmoqdan foydalanish tartibining buzilishi, tashqi (begona) dasturlarni qo‘llash faktini (izlari) belgilash);

– hisoblash tizimining holati va xususiyatlarini ma’lumot tashuvchilaridagi axborotga asosan aniqlash (masalan, raid-massivlar, qattiq disklar, floppy-disklar, CD-rom, zip-to‘plovchilar va h.k.)

– mexanizm strukturasi va tarmoqdagi hodisa oqibatlarini natijalarga asosan aniqlash (masalan, ruxsatsiz kirish, zararli funksiyalarning tarmoqda tarqalish mexanizmi ssenariysi);

– ma’lum apparat-dasturiy hisoblash tizimi vositalaridan foydalanish va buning natijasi orasidagi aloqani aniqlash.

Sud amaliyotini tahlil qilgandan so‘ng, bugungi kunda dasturiy-kompyuter ekspertizasining asosiy vazifalari quyidagilardan iborat degan xulosaga kelinadi:

– umumiy tashxis va dasturiy ta’minot vazifalarini belgilash;

– dasturiy ta’minot mahsulotining algoritmini foydalanuvchining tegishli ruxsatnomasisiz tanadagi imkoniyatlarini (modifikatsiya qilish, blokirovkalash, nusxalash) aniqlash uchun tashxis etish;

– zararli dasturlar belgilarini aniqlash;

– mahsulot kelib chiqishining bir umumiy manbaini aniqlash.

Shuni ta’kidlash kerakki, yuqorida keltirilgan kompyuter-texnik ekspertiza masalalarini hal qilish uchun dasturiy ta’minot, algoritmlashtirish, ma’lumotlar bazalarini yaratish, dasturiy ta’minotni tasniflash va shu kabi sohalarda maxsus bilimlarga ega bo‘lish lozim.

Ekspert dasturlari. Ekspertiza davomida kompyuter ma’lumoti tashuvchisini tahlil qilish uchun qo‘llaniladi.

Keng tarqalgan ekspert dasturlari:

– ProDiscover dasturlari oilasi.

– SMART (Storage Media Analysis Recovery Toolkit).

– «AccessData» Encase firmasinign Forensic Toolkit (FTK)– mutaxassis tizimi

– SATAN (System Administrator Tools for Analyzing Networks) -UNIX OT uchun kompyuterdan to‘liq ma’lumotni olish vositasi.

– Helix - Linux asosidagi o‘rnatiluvchi kompakt diskdagi mutaxassis to‘plamidir.

5.4. Tadqiq qilish turlari va toifalari

1. **Texnik tizimlarning apparat ekspertizasi** jinoyatga oid moddiy axborot tashuvchilarining to‘g‘ri ishlashini o‘rganishga qaratilgan. Ushbu bosqichdagi asosiy masalalari quyidagilardir:

- uskunaning texnik va funksional xususiyatlarini aniqlash;
- texnik holatni tekshirish;
- apparatdan foydalanish natijalari asosida hodisaning sxemasi va shartlarini belgilash;
- qurilmadan foydalanish va buning natijalari o‘rtasidagi bog‘liqlikni aniqlash;
- xronologiyani yaratish;
- topilgan funksiyalar bo‘yicha apparatning spetsifikatsiyasi.

2. **Dasturiy ta’minotga asoslangan kompyuter-texnik ekspertizasi (KTE)** jinoyat yoki fuqarolik tekshiruvlarida haqiqatni aniqlash uchun kompyuter dasturlarini ishlab chiqish va qo‘llashning

qonuniyatlarini o‘rganadi. Ushbu bosqichda amalga oshirilgan algoritmning funksional vazifalari va funksional xususiyatlarini, kompyuter tizimining dasturiy xususiyatlarini va hozirgi holatini o‘rganish kerak.

3. **Ma’lumotlar tahlili -** ekspert kompleksidagi asosiy baholash, negaki u dalillar bazasini to‘liq holatini taqdim etish uchun imkon beradi. Bunga kompyuter ma’lumotlariga taalluqli diagnostika va identifikatsiyalash masalalarini bajarish orqali erishiladi. Ushbu bosqichning maqsadlari foydalanuvchi yoki axborot jarayonlarini tashkil qilish dasturlari tomonidan ishlab chiqarilgan (yaratilgan) kompyuter tizimi tomonidan tayyorlangan axborotlarni qidirish, aniqlash, tahlil qilish va baholashni o‘z ichiga oladi.

Tadqiqot usullari. Bugungi kunda kompyuter ekspertizasi metodologiya shakllanish bosqichini boshidan kechirmoqda. Ammo apparat, dasturiy ta’minot va ma’lumotlar bazalari tadqiqot usullarini allaqachon ajratish mumkin.

Apparatning funksionalligini tekshirish vositalari quyidagilar:

- funksiyalarni almashtirishning matematik usullari;
- BIS va BIS xotirasini sintez qilish va qurish usullari;
- mikroprosessorning me’moriy usullari;
- raqamli tugunlarni sintez qilish usullari;
- audio va video media uchun signalni ishlash usullari;
- optik usullar va boshqalar.

Dasturiy ta’minotni tadqiq qilish protseduralari o‘zaro tekshiruv uchun taqdim etilgan obyekt turiga qarab tasniflanishi mumkin:

- yuk modullarini va dastur algoritmlarini o‘rganish usullari;
- boshlang‘ich kodni o‘rganish.

Qimmatli axborotni (ma’lumot) tekshirish usullari quyidagi kompleks ko‘rinishida bo‘lishi mumkin:

- erkin foydalanish va ma’lumotlarni qidirish usullari;
- tiklash va arxivlash usullari;
- axborotni manipulyatsiya qilish usullari (tahrirlash, ko‘chirish, nusxalash).

Kompyuter-texnik ekspertizaning maxsus usullariga ma’lumotlarni qayta ishlashni tarqatish; iyerarxiyalash; topologiya; marshrutlash; kommutatsiya va boshqalar kiradi. Har qanday aloqa (mobil aloqa, sun’iy yo‘ldosh, magistral, simsiz va boshqalar) sinovlardan o‘tgan hollarda telekommunikatsiya usullari oldinga chiqariladi:

1. Protokollash.

2. Axborot uzatishning raqamli va analog usullari.
3. Ma’lumotlarni siqish va himoya qilish usullari.
4. Kodlash va dekodlash.
5. Signallarning modulyatsiyasi va demodulyatsiyasi va h.k.

Eng ishonchli tadqiqot usullari orasida kompyuter tarmog‘i muhitidagi tajriba deb atash mumkin. Dasturiy internet-kiritmalarni o‘rganish davomida olib boriladi. Internet tarmog‘ining ishtirokchilari o‘rtasida aloqaga taqlid qilish uchun mo‘ljallangan bir necha kompyuterlardan iborat internet tarmoqg‘i segmenti hosil qilinadi.

Ulardan birinchisi muayyan provayder orqali bog‘langan obyekt, ikkinchisi - ushbu provayderning serveridir. Uning yordami bilan, dasturiy ta’minot yorlig‘i orqali Internetdagi boshqa kompyuterlar haqidagi internet ma’lumotlarini topish mumkin.

Ikkinchi kompyuter server domeniga, uchunchisi foydalanuvchiga taqlid qiladi. Uning manzili bo‘yicha kiritma dasturidan olingan ma’lumotlar uzatiladi. Shu tarzda, foydalanuvchi yoki boshqa axborot haqidagi ma’lumotni uning kompyuteridan boshqa tashuvchi vositalarida qabul qilinishini aniqlash mumkin. Yuqoridagi barcha usullar hech qachon yolg‘iz foydalanilmaydi. Ishonchli va malakali natijaga erishish uchun faqatgina kompleks yondashuvni amalga oshirish mumkin.

Kompyuter mutaxassisi qanday muammolarni hal qilish kerak? Sud kompyuter-texnik ekspertizasi (SKTE) tadqiq qilishchi (yoki sud) tomonidan taklif qilinishi mumkin, lekin uni mas’ul mutaxassis yoki mutaxassislik tashkiloti tomonidan amalga oshiriladi. Tadqiqot protokoli ishni tasdiqlash dalili bo‘lib xizmat qiladi. Fuqarolik-huquqiy sohadasi sud, bir tomon yoki notarius so‘rovi bo‘yicha ekspertiza tayinlanishi mumkin.

Mutaxassis-ekspert oldida turgan savollar:

1. Sudda foydalanilishi mumkin bo‘lgan ma’lumotlarning o‘rganilayotgan obyektlarida mavjud bo‘lishi (maxfiy yoki ochiq).
2. Mutaxassislik obyektlarini muayyan maqsadlar uchun ishlatish (masalan, tarmoqqa ulanish uchun).
3. O‘rganish obyekti bilan qandaydir harakatni amalga oshirish ehtimoli.
4. Kompyuter dasturlarining xususiyatlari, shu jumladan ularning zararli dasturlardan foydalanishi.

5. Dasturlar, hujjatlar, kompyuter foydalanuvchilarini aniqlash.

Shu bilan birga, bu holatda ekspertning vakolatiga kirmaydigan bir nechta fikrlar mavjud, shuning uchun protokolda ularning mavjudligi noto‘g‘ri deb hisoblanadi. Bunga quyidagilar kiradi:

1) Dasturiy ta’minotning o‘ziga xosligi (litsenziyalash).

2) O‘rganilayotgan obyektlaridan foydalangan holda amalga oshirilgan harakatlarning qonuniyligi.

3) Apparatlar, vositalar va dasturlarning narxi.

4) Topilgan matnlar, hujjatlar va boshqalar.

Ekspert bahosi sudda e’tirof etilishi uchun barcha qoidalarga muvofiq amalga oshirilishi lozim. Bunday holatlarda xatoga yo‘l qo‘ymaslik kerak.

Ekspert bahosi bo‘yicha ko‘proq uchraydigan savollar. Ishning barcha sharoitlarini aniqlash uchun, bugungi kunda mutaxassis quyidagi savollarga javob topishi kerak:

✓ Ushbu kompyuter vositasi Internetda ishlashining isboti bormi?

✓ Internet tarmog‘iga qanday vosita yordamida ulaniladi?

✓ Tayyor internet-aloqaning mavjudligi, ularning xususiyatlari (yaratilgan sana, foydalanuvchi nomlari, parollar, provayder koordinatalari va boshqalar).

✓ Masofaviy erkin foydalanish dasturlari va aloqa protokollari parametrlarining mazmuni.

✓ Ushbu kompyuter foydalanuvchisi qaysi saytlarga tashrif buyurdi?

✓ Elektron to‘lovlar yoki kredit kartochkalari haqida ma’lumotlar mavjudligi.

✓ Elektron pochta xabarlari (qabul qilingan va yuborilgan).

✓ Maxsus aloqa dasturlari orqali yuborilgan xabarlar, ularning mazmuni.

5.5. Tadqiq qilish jarayoni

Tadqiq qilish davomida mutaxassislar quyidagi harakatlarni amalga oshiradilar:

1. Vaziyatni baholash - tadqiq qilishning ko‘lamini va olinadigan xatti-harakatlarini tahlil qilish.
2. Ma’lumotni to‘plash, dalillarni himoya qilish, to‘plash va saqlash.

3. Ma’lumotlarni tahlil qilish, real qiziqish uyg‘otuvchi, keyinchalik ish jarayonini tushunishga imkon beruvchi hodisa va raqamli dalillarni tahlil qilish va o‘zaro bog‘lash.

4. Amalga oshirilgan tadqiq qilish bo‘yicha hisobot tayyorlash - axborotni to‘plash va tashkillash, yakuniy hisobotni tayyorlash.

Tadqiq qilishni boshlashdan oldin tadqiq qilish jarayoniga turtki berish kerak. Avval siz advokatlarni tajovuzkorning ma’muriy (jinoiy) ishi bilan shug‘ullanishi uchun jalb qilish masalasini aniqlashtirishingiz kerak. Agar ha bo‘lsa, huquq tartibot idoralarini jalb qilish lozim. Biroq bu tadqiq qilishning keyingi bosqichlarida amalga oshirilishi mumkinligini yodda tutish zarur. Birinchi navbatda, tajovuzkorlar tomonidan keltirilishi mumkin bo‘lgan kelajakdagi zararni bartaraf etish kerakligini anglash kerak. Albatta, davlat xavfsizligi manfaatlariga xilof bo‘lmasa, eng muhimi, tashkilotni mumkin bo‘lgan zararlardan himoya qilishdir.

Rahbariyatni xabardor qilish. Agar xavfsizlik siyosati Insident ruxsatini o‘z ichiga olmasa, korxona boshqaruvidan Insidentning ichki tekshiruvi uculiga ruxsat olish talab qilinadi. Bunday holatda vaziyatni to‘liq baholash va keyingi bosqichlarni aniqlash kerak. Buning uchun quyidagilar bajariladi.

a) Agar tashkilotda muayyan Insidentga javob berish siyosati bo‘lmasa, boshqaruvni yozma ravishda xabardor qilish va vakolatli shaxsdan kompyuterni tadqiq qilish qilish uchun yozma ruxsat olish kerak.

b) Tadqiq qilish davomida u bilan bog‘liq barcha harakatlarni hujjatlashtirish kerak. Insident davomida yuz bergan barcha hodisalar va unga javobning qonuniy tafsilotiga ega bo‘lishingiz zarur. Tadqiq qilish jarayonidagi harakatlarni tasvirlash uchun keyinchalik bu hujjat ishlatilishi mumkin.

c) Insident kontekstiga ko‘ra va davlat xavfsizligiga tahdid bo‘lmaganda tashkilotni kelajakdagi zararlardan himoyalash asosiy vazifaga aylanadi. Tashkilotning xavfsizligi kafolatlangandan so‘ng, ishni tiklash va Insidentni tekshirish kerak.

Sizning yechim va dalillaringiz sud davomida shubhaga olinishi mumkin, negaki kompyuter dalillarini to‘plash jarayoni qiyin bo‘lib, turli usullar turli natijalarni berishi mumkin.

Siyosatlar va protseduralarga umumiy nazar. Kompyuter tadqiq qilishiga o‘tishda, jarayon davomida murojaat qilinishi mumkin

bo‘lgan korxonada qabul qilingan siyosat va protseduralarni tushunish o‘ta muhimdir. Quyidagi muhim masalalarga e’tibor bering.

1. Tadqiq qilish uchun qonuniy vakolatlaringiz bormi?
2. Maxfiy ma’lumot bilan ishlashni yorituvchi qoidalar tashkilotda qabul qilinganmi?
3. Insident yuzaga kelgan taqdirda ichki tekshiruv o‘tkazish qoidalalri ushbu siyosat va protseduralarda tasvirlanganmi? Sir emaski, ko‘plab tashkilotlarda bunga mos siyosat va protseduralar mavjud emas yoki ko‘rib chiqilmagan yoki yuristlar bilan muhokama qilinmagan. Bundan tashqari, xodimlar va tashrif buyuruvchilarning hammasi ham bulardan xabardor emas. O‘z vakolatlaringiz xususida ishonchingiz komil bo‘lmasa, ma’muriyat yoki yuristlar bilan maslahatlashing.

Tadqiq qilish natijalarini noto‘g‘ri qayta ishlash bilan bog‘liq bo‘lgan muammolarni bartaraf etish uchun advokatlar bilan maslahatlashing. Bunday muammolarni keltirib chiqaradigan omillar orasida quyidagilar bo‘lishi mumkin:

- jabrlangan mijozlarning shaxsiy ma’lumotlari;
- har qanday davlat qonunlarining buzilishi;
- elektron xabarlarni qo‘lga kiritganlik jinoiy yoki ma’muriy javobgarlik;
- ommaviy bo‘lmagan ma’lumotlarni ko‘rish. Agar tadqiq qilish davomida to‘g‘ridan to‘g‘ri qo‘llanilsa, mijoz maxfiyligini xavfga solishi mumkin bo‘lgan ma’lumotlar hujjat tadqiq qilishiga bog‘liq bo‘lak sifatida ommaga ochiq bo‘lishi mumkin.

Kelajakda quyidagilar mijoz ma’lumotlarning maxfiyligini ta’minlash uchun zarur:

- barcha ma’lumotlar ishonchli tarzda saqlanishi va erkin foydalanishi cheklanishi kerak;
- tadqiq qilish oxirida, barcha hujjatlar, shu jumladan, advokatlar bilan kelishilgan yoki qonunga muvofiq barcha ma’lumotlar kuchli nazorat ostida saqlanishi kerak. Agar jinoiy ishning potensial bo‘lagi bo‘lsa – qonun tartiboti organlari bilan maslahatlashish lozim.

Da’vo yuzaga kelgan bo‘lgan taqdirda, barcha dalillarning raqamli nusxalari ehtiyotkorlik bilan saqlanishi kerak. Agar siz dalillarni saqlashni kafolatlamasangiz, tadqiq qilish davomida topilgan

dalillar ishonchli ekanini kafolatlamaysiz. Dalillarni saqlash tekshiriladigan hujjatlarning mavjudligi bilan ta’minlanadi.

Tadqiq qilish guruhini tuzish. Ichki kompyuter tekshiruvini muvaffaqiyatli o‘tkazish uchun Insidentga javob berish guruhini tuzish kerak. Haqiqatdan ham tadqiq qilish qilishga ehtiyoj tug‘ilishidan oldin, guruhni oldindan tuzish yaxshidir. Guruh a’zolari bunday tekshiruvlarni o‘tkazish qobiliyatiga ega bo‘lishi muhimdir. Quyidagilarni e’tiborga olish lozim.

✓ Tadqiq qilish qanday bo‘lishini tushunuvchi vakolatli xodimlarni aniqlash. O‘quv kurslarida o‘qish buning uchun ideal bo‘ladi. Sud muhokamasi o‘tkaziladigan bo‘lsa, jarayonni amalga oshirgan tadqiq qilish xodimining qobiliyatlari va malakasi yaxshilab tekshiriladi.

✓ Tadqiq qilish guruhiga a’zolar tayinlang va ularning mas’uliyatini aniqlang.

✓ Jamoa a’zolaridan birini texnik boshqaruvchi sifatida belgilang.

Odatda texnik boshqaruvchi tadqiq qilishlarda ishtirok etish tajribasi va yetarli texnik bilimlarga ega bo‘lishi kerak. Tadqiq qilish guruhining a’zolari gumondorlardan ko‘ra ko‘proq malakali bo‘lishi kerakligini unutmang.

1. Tadqiq qilish guruhi a’zolari ma’lumotlarini va shaxsiy xavfsizligini himoya qilish uchun jamoani yashirin saqlash kerak.
2. Tadqiq qilish o‘tkazilishi holatida ish guruhining har bir a’zosi muammoni hal qilish uchun yetarli ko‘nikmaga ega ekanligi ta’minlanishi kerak. Ushbu punkt tashqi ekspertlarning tadqiq qilish o‘tkazish uchun jalb qilinishida juda muhimdir.

Vaziyatni to‘liq baholash. Tegishli ishlarni birinchi o‘ringa qo‘yish va tadqiq qilish guruhiga mablag‘ ajratish uchun vaziyatni batafsil baholash kerak. Ushbu baholash Insidentning tashkilotning faoliyatiga hozirgi va potensial ta’sirini belgilaydi, ta’sir ostidagi infratuzilmani aniqlaydi va imkon qadar vaziyatni baholaydi. Shu bilan birga, bu ma’lumot tegishli ish yo‘nalishini tezda aniqlab olishga imkon beradi.

Vaziyatni to‘liq baholash uchun quyidagi harakatlar talab etiladi.

- Barcha potensial xavflar, potensial jalb etilgan tomonlar, va iloji bo‘lsa, shubha ostidagi tomon to‘g‘risida ma’lumotni o‘rganish

- Tashkilotga potensial ta’sirni o‘rganish. Mijoz ma’lumotlari, moddiy holati yoki tashkilotning maxfiy ma’lumotlari Insidentda ta’sir ostiga tushganmi yoki yo‘qligini baholash. Bu baholash axborot texnologiyalari va axborot xavfsizligi xizmati vakolatining chegarasidan tashqarida bo‘lishi mumkin va kompaniya boshqaruvi hamda yuristlar yordamida amalga oshirilishi kerak.
- Tadqiq qilish davomida tashkilot faoliyatiga ta’sirini tahlil qilish va Insident asoratlarini to‘liq yo‘q qilish uchun ketadigan resurslar, to‘xtalish vaqti, zararlangan qurilmalar narxini sanang, daromaddan yo‘qotishlar va maxfiy ma’lumotni tarqatish narxini aniqlang.
- Moddiy bo‘lmagan yo‘qotishlarni - tashkilot nufuziga ta’sir va boshqalarni tahlil qiling. Ushbu yo‘qotishlarni baholash axborot texnologiyalari va axborot xavfsizligi xodimlari vakolatidan tashqarida bo‘ladi hamda yuristlar va boshqa bo‘limlardagi xodimlar bilan birga boshqaruv tomonidan bajariladi.

Insident ta’siriga tushgan tarmoq infratuzilmasi va kompyuterlarni aniqlash, tahlil qilish va hujjatlashtirish uchun quyidagilarni amalga oshirish kerak:

1. Insidentda qatnashadigan zararlangan kompyuterlarning soni, turlarini va rollarini aniqlash.
2. Tarmoq topologiyasini, shu jumladan serverlar, tarmoq apparatlari, xavfsizlik devorlari va internet aloqalari haqida batafsil ma’lumotni

tekshirish.

3. Tashqi xotira qurilmalarini aniqlash.
4. Kompyuter tarmog‘iga ulangan masofadagi kompyuterlarni aniqlash.
5. Zarurat paydo bo‘lsa tarmoq trafikini qo‘lga olish. Tarmoqda hali ham shubhali trafik mavjud bo‘lsa, ushbu turdagi tahlil qilish.
6. Tadqiqot tarkibiga kirgan kompyuterlarda ilovalar va operatsion tizimlarning holatini o‘rganish uchun vositalardan foydalanish.

Bunday holda, Windows, Windows Sysinternals PsTools jurnal

fayllari foydali bo‘ladi.

7. Ta’sir ostidagi fayllar va dastur serverlarini tadqiq qilish va hujjatlashtirish uchun Windows Sysinternals asboblar

to‘plamidan foydalanish: PsTools, PsFile, ShareEnum va Windows log fayllari.

Vaziyatni to‘liq anglash uchun quyidagilarni amalga oshirish lozim:

- Vaqtinchalik trafikni tuzish. Bu global inqirozlar uchun ayniqsa muhimdir. Ushbu hujjatda ish stansiyalaridagi sana va vaqt hamda Windows Server xizmatining vaqti orasida yuzaga kelishi mumkin bo‘lgan nomuvofiqliklar bo‘lishi kerak.
- Insidentga jalb etilgan shaxslar doirasini aniqlang va ular bilan suhbatlashish. Bu vaziyatni tushunish uchun juda muhimdir.
- Intervyudagi barcha natijalarni hujjatlashtiring. Keyinchalik ular vaziyatni to‘liq tushunish uchun talab qilinadi.
- Tarmoqning tashqi va ichki vositalaridagi, masalan, hujum yo‘lida joylashishi mumkin bo‘lgan tarmoq himoyasi tizimi va marshrutizatorlaridagi ma’lumotni (jurnal fayllari) tiklash va saqlash.
- Windows Sysinternals Whois yordamida omma uchun ochiq ma’lumotni, masalan, ip-manzil va domen nomi turidagi axborotni hujumchini aniqlash uchun qo‘lga kiritish mumkin.

Dalillarni to‘plash. Raqamli dalillar mahalliy holatda yoki tarmoq orqali amalga oshiriladi. Biroq mahalliy ma’lumotlarni yig‘ish har doim ham mumkin emas. Tarmoqda ma’lumotlarni yig‘ish taqdirida to‘plangan ma’lumotlar turi va sarflangan kuch hisobga olinishi kerak.

Ma’lumotlarni to‘plashning tavsiya etilgan jarayoni:

1. To‘plangan dalillarning haqiqiyligini tasdiqlaydigan aniq hujjat yaratish. Tadqiq qilish jarayonida har qanday potensial qiziqarli elementlarga e’tibor berish va keyinchalik muhim deb hisoblash mumkin bo‘lgan har qanday xatti-harakatlarni qayd etish muhimdir. Muvaffaqiyatli tekshiruvning kalitlari quyidagilardan iborat:

1) Kim harakatni amalga oshirdi va nima uchun?
2) Ular shu yo‘l bilan nimaga erishmoqchi bo‘ldilar?
3) Bu harakat qanday amalga oshiriladi?
4) Qanday vositalar va tartiblar ishlatilgan?
5) Harakat qachon (sana va vaqt) bajarilgan?
6) Qanday natijalarga erishildi?

2. Zarur tadqiq qilish usullarini aniqlash. Odatda, avtonom va interaktiv usullarning kombinatsiyasi qo‘llaniladi.

✓ Avtonom tekshiruvlar o‘tkazishda, dastlabki dalillarning yagona nusxasi bo‘yicha qo‘shimcha tahlillar amalga oshiriladi. Avtonom

tekshiruv usuli iloji doim qo‘llaniladi, chunki bu asl dalillarga zarar yetkazish xavfini kamaytiradi. Biroq ushbu usulni faqat tegishli nusxa ko‘chirish mumkin bo‘lgan va ba’zi bir quvvatga bog‘liq ma’lumotlarni yig‘ish uchun ishlatib bo‘lmaydigan holatlarda foydalanish mumkinligini hisobga olish kerak.

✓ Avtonom tekshiruv o‘tkazishda tahlil asl operatsion dalillar asosida amalga oshiriladi. Dalillarni o‘zgartirish xavfi tufayli tadqiq qilishga jalb qilingan xodimlar ayniqsa ehtiyot bo‘lishi kerak.

3. Potensial ma’lumot manbalarini hujjatlashtirish va aniqlash, bunga quyidagilar kiradi:

- serverlar; ma’lumotlar server roli, log fayllari, ma’lumotlar fayllari, ilovalarni o‘z ichiga oladi;
- tashqi va ichki tarmoq qurilmaning log fayllari;
- ichki apparat komponentlari (masalan, tarmoq adapterlari);
- tashqi portlar - Firewire, USB va PCMCIA;
- saqlash uskunalari, shu jumladan qattiq disklar, tarmoq uskunalari, olinadigan media;
- portativ mobil qurilmalar - Pocket PC, Smartphone i MP3-pleyerlar.

4. Quvvatga bog‘liq ma’lumotni yozishda ma’lumotlarni yig‘ish tartibi diqqat bilan ko‘rib chiqilishi kerak. Shuni e’tiborga olish kerakki, quvvat o‘chirilganda, quvvatga bog‘liq dalillar osongina yo‘qoladi .

5. Ma’lumotlar to‘plashning quyidagi usullaridan foydalanish zarur:

- Agar biron-bir ichki xotira qurilmasini olib tashlash kerak bo‘lsa, barcha quvvatga bog‘liq ma’lumotlar aniqlanganligini tekshirishingiz kerak, shundan so‘ng kompyuterni o‘chirish lozim.
- Saqlash qurilmasini olib tashlash yoki ma’lumotlarni belgilash uchun o‘z tizimingizdan foydalanishni hal qiling. Ehtimol, saqlah qurilmasini apparat bilan mos kelmasligi sababli o‘chira olmasligingiz mumkinligini inobatga oling.
- zaxiradagi ma’lumot tashuvchi vositalarda dalillarning yagona nusxasini yaratib, asl nusxasini himoyalang. Barcha keyingi ma’lumotlarni tahlil qilish asl nusxada emas, balki ushbu nusxada amalga oshirilishi kerak.
- Saqlash moslamalarini hujjatlashtirishda konfiguratsiya ma’lumotlarining mavjudligiga ishonch hosil qiling. Ishlab chiqaruvchi

va jihozlar modeliga, ulanish sozlamalari, qurilma hajmiga, interfeysning turiga va diskdagi holatga e'tibor bering.

6. To'plangan ma'lumotlarni tekshirish. Agar iloji bo'lsa, to'plangan ma'lumotlarning original bilan bir xil bo'lishini ta'minlash uchun nazorat summalari va raqamli imzolarni yarating. Ba'zi hollarda (masalan, ma'lumotni saqlash vositalarida nosoz sektor mavjud bo'lsa) mutlaq nusxasini yaratishning ilojisi yo'q. Biroq siz mavjud vositalar yordamida olinishi mumkin bo'lgan eng yaxshi nusxasini olganingizga ishonch hosil qiling.

Saqlash va arxiv. Dalillar to'planib, kanallar hosil qilib bo'lingach, butunligini ta'minlash maqsadida arxivlash va ularni saqlash juda muhimdir.

Ma'lumotlarni saqlash va arxivlashning eng ishonchli usullarini sanab o'tamiz.

1. Ma'lumotlarni jismonan xavfsiz joyda saqlash.
2. Ma'lumotlarga jismoniy va tarmoqdan foydalanish ochiqligini hujjatlashtirish.
3. Tasdiqlanmagan shaxslarning tarmoq yoki boshqa vositalar orqali dalillarga kirishiga imkon bermaslik.
4. Dalilarni saqlovchi vositalar joylashgan xonalar va uskunalarni elektromagnit maydon va statik elektr ta'siridan saqlash.
5. Tadqiq qilish davomida kamida ikki nusxadagi dalillarni to'plash. Shu bilan birga, nusxalaridan biri asosiy binoning tashqarisida xavfsiz joyda saqlanishi kerak.
6. Dalillar ham moddiy shaklda (masalan, seyfga joylashtirilgan), va ham raqamli shaklda (masalan, parol axborot vositalari uchun tayinlangan) saqlanganligi.
7. Barcha dalillarni saqlash jarayonini hujjatlash.
8. Quyidagi ma'lumotlarni o'z ichiga olgan nazorat jurnalini yaratish:
   - dalillarni tadqiq qilish qiluvchi shaxsning nomi;
   - dalil bilan ish boshlash sanasi va vaqti;
   - uning omborga qaytarilgan sanasi va vaqti;

5.6. Forensic Toolkit raqamli sud-tibbiyot ekspertizasi

Forensic Toolkit (Cud vositalar to'plami), ***FTK*** – AccessData tomonidan ishlab chiqilgan kompyuter ekspertiza dasturlari. Ushbu dastur qattiq diskni skaner qilish imkonini beradi, bu esa turli

ma’lumotlarni topish jarayonini osonlashtiradi. Masalan, o‘chirilgan elektron pochta manzillarini yoki parol lug‘ati sifatida foydalanish uchun matn satrlari uchun diskni topish.

Vositalar to‘plami «The FTK Imager» (FTK tasvirini) disk ko‘rinishini hosil qilish avtonom dasturini ham o‘z ichiga oladi. U qattiq disk tasvirini keyinchalik tiklashning imkoni bo‘lgan fayllarda yoki segmetnlarda saqlovchi oddiy, ammo foydalanishi qulay dasturdir. Bundan tashqari xesh qiymatini hisoblaydi va fayllarni yopishdan oldin ma’lumotlarning butunligini tekshiradi. Natija - bir necha formatlarda saqlanishi mumkin bo‘lgan obraz fayllari, jumladan, xom DD ma’lumotlari.

Cud vositalar to‘plami (FTK) raqamli kriminalistikada qo‘llaniladigan dunyoda tan olingan standart dasturiy ta’minot bo‘lib, tezkor, barqaror va qulay foydalanish uchun mo‘ljallangan sud tomonidan raqamli tadqiqotning yagona tan olingan yechimidir. O‘zining intuitiv interfeysi, pochta tahlili, ma’lumot tushunchasining o‘zgaruvchanligi va turg‘unligi bilan dunyoda tan olingan FTK o‘zining strukturasini kengaytirish imkonini beradi.

Forensic Toolkit (FTK) dasturiy ta’minoti ishlab chiqarish bilan shug‘ullanuvchi sud ekspertlari uchun ajralmas vositadir. Forensic Toolkit - butun dunyo bo‘ylab sud ekspertlari sohasida dunyo standarti tomonidan tan olingan keng qo‘llaniluvchi kompyuter ekspertizasi vositasi. Dastur ma’lumotning sud-tibbiyot jihatdan aniq va keng qidiruvini amalga oshiradi, moslashtirish yo‘li bilan parollarni deshifrlaydi va buzadi, raqamli kriminalistika ekspertizalarini o‘tkazishda muhim asbob hisoblanadi. Forensic Toolkit dasturiy ta’minot muhitida ishlash vaqtini tejash orqali dasturda ishlashni osonlashtiradigan shaxsiy sozlash imkoniyati bilan intuitiv interfeysga ega.

Dastur yirik kompaniyalarda ishlatilishsh uchun o‘lchov qobiliyatiga ega bo‘lgan ma’lumotlarni tezkor tahlil qilish imkonini berishi tufayli tashkilotda muayyan ehtiyojlar bo‘lgan taqdirda kompyuter ekspertizasi ko‘lamini yanada kengaytirish imkoniyatini beradi. Sud-meditsina vositasi bugungi kunda kompyuter va texnik mutaxassislik uchun eng zamonaviy dastur hisoblanadi. Ilgari, odatda, faqat boy kompaniyalar huquqni muhofaza qilish idoralarida, ta’lim muassasalarida, davlat idoralarida, korporatsiyalarda ishlovchi xodimlar yoki kompyuter xizmatini ko‘rsatuvchilar tomonidan qo‘llanila oluvchi dasturdan foydalana olardi. Bugun esa, hatto kichik firmalar

bunday dasturlardan foydalanishi mumkin. Bu ushbu dasturiy ta’minotning yana bir afzalligidir.

AccessData Forensic Toolkit - kompyuter tekshiruvlarini o‘tkazish uchun dasturiy ta’minot, xotira dampining tahlilini ta’minlaydi, kuchli qidiruv vositasidan foydalanadi, arxiv ma’lumotlarini oladi va sud-ekspertizaning bir qismi sifatida to‘liq kompyuter ishini olib boradi. FTK parolni tiklash va parolni deshifrlash uchun AccessData firmasi mahsuloti bilan integrallashadi (Password Recovery Toolkit).

FTK xususiyatlari:

1) Ishlatishdada qulaylik:

a) Stellent’s Outside In Viewer Technology yordamida 270 dan ziyod fayllar formatlari va kodirovkalarni ko‘rib chiqish.

b) Ekspertiza paytida bajarilgan barcha harakatlar va operatsiyalarning natijalarini qayd etadi.

c) Tegishli hisobotlarni ishlab chiqaradi.

d) Tadqiq qilingan media bo‘yicha matnli ma’lumotlarning to‘liq indeksatsiyasi kontekstli qidirish natijalarini darhol namoyish etish imkonini beradi.

ye) JPEG formatidagi grafik tasvirlar va veb-sahifalar matn elementlari - fayllar uchun mukammal qidiruv rejimi.

f) Ko‘rsatilgan parametrlarga ko‘ra axborotni qidirish.

g) Axborotlarni avtomatlashtirilgan tahlil qilishda foydalanish uchun ularni ekspertizadan o‘tkazish odatiga ega bo‘lgan fayllar kutubxonasini (hashsets) yaratish.

2) Fayl tizimlari va ommaviy axborot vositalarining nusxalari bilan ishlash:

a) Quyidagi fayl tizimlarida ishlashni qo‘llab-quvvatlaydi: NTFS, siqilgan NTFS, FAT 12/16/32 i Linux ext2 i ext3.

b) Quyidagi pochta mijozlari dasturlarini qo‘llab-quvvatlaydi: Outlook, Outlook Express, AOL, Netscape, Yahoo, Earthlink, Eudora, Hotmail df MSN.

c) Elektron pochta ma’lumotlar bazasidan elektron pochta yoki kiritmalarni ko‘rish, qidirish, chop etish va eksport qilish imkonini beradi.

d) Qoralamalar papkasida joylashgan yoki o‘chirilgan elektron pochta xatlarini qayta tiklaydi.

e) Quyidagi dasturlar yaratgan arxivdan fayllarni avtomatik ravishda chiqaradi: PKZIP, WinZip, WinRAR, GZIP i TAR.Known File Filter (KFF):

f) NIST va Hashkeeper tomonidan yaratilgan Hash Sets ma'lumotlar bazasini qo'llab-quvvatlaydi.

g) O'zining bazalarini yaratadi.

Registry Viewer quyidagilarni ta'minlaydi:

✓ Axborotga to'g'ridan-to'g'ri kirish va axborot tashish vositalaridagi shifrlangan ma'lumotlarning parolini deshifrlash

✓ Tizim retstri fayllarini ko'rish.

✓ Hisobotni yaratish.

✓ Ushbu dastur boshqa AccessData dasturiy mahsulotlar bilan mos keladi.

Forensic Toolkit (FTK)ning xususiyatlari:

Kompyuter texnik ekspertizasi uchun keng qamrovli yechim. Tasvir yaratish, ro'yxatga olishni tahlil qilish, tekshiruvlarni olib borish, fayllarni deshifrlash, parollarni buzish, steganografiyani tanib olish va hisobotlarni tuzish. 100 dan ortiq ilovalar uchun parollarni tiklash, tarmoqdagi to'xtashlar vaqtida parol shifrini aniqlash va lug'at bo'yicha hujum amalga oshirish uchun protsessorning hisoblash kuchini qo'llash. 45-million xeshlardan iborat xesh kutubxonasi.

Katta korxona arxitekturasi. Juda katta, eng murakkab ma'lumotlar ketma-ketligini qo'llab-quvvatlash. Dasturning moduli bir-biridan mustaqil ekan, muvaffaqiyatsizlik taqdirida ishning natijalari yo'qolmaydi. Ishning rezerv nusxasini yaratish va arxivlash mumkin. Har bir FTK nusxasi tarqalgan qayta ishlashni amalga oshirish uchun 4 ta agentni o'z ichiga oladi: 1- mutaxassis mashinasida, qolgan 3 shaxsiy kompyuterlarda joylashgan (xohishga ko'ra mutaxassislar sonini oshirish mumkin). Tarqatish jarayoni kuchli apparat va tarmoq texnologiyalarini talab qiladi. I/O operatsiyalari juda jadal bo'lgani uchun, axborotni qayta ishlash tez diskni talab qiladi. Bundan tashqari, Processing Manager ishlovchi mashina guruhdagi eng katta tezlikka (CPU) ega bo'lishi lozim. Dasturiy yechim laboratoriya imkoniyatlarini qo'shib osonlik bilan kengaytiriladi. Bu hukumat tuzilmalari va huquqni muhofaza qilish organlari uchun muhimdir.

Kuchli va tez qayta ishlash vositalari.

1. Tezkor javob qaytarish xususiyatiga ega grafik interfeys.

2. Tarqatilgan qayta ishlash vaqtini sezilarli darajada kamaytirish va katta hajmdagi ma’lumotlarni tahlil qilish uchun 3 tagacha kompyuterni ishlatishga imkon beradi.

3. Ko‘p protsessorlik va ko‘p tarmoqlilikni qo‘llab-quvvatlaydi.

4. "Bekor qilish jarayoni / to‘xtatib turish / davom ettirish" variantlari.

5. CPU ga yuklashni taqsimlash.

6. Qayta ishlash tugallanishi haqida elektron pochta orqali xabar qilish imkoniyati.

7. Ma’lumotlarni tanlashning rivojlangan mexanizmi kerak bo‘lmagan ma’lumotni tashlab yuborish uchun tanlangan/tanlanmagan maydondan quyidagi talablarga javob beruvchi ma’lumotni tanlaydi: fayl hajmi, ma’lumotlar turi, va hokazo.

8. dt Search bilan yaxshilangan integratsiya tezlik bilan indekslash va qidiruv natijalarini olish imkonini beradi.

Operatsion ma’lumotlarni oldindan ko‘rish, yig‘ish va tahlil qilish. Qurilmalardan, mantiqiy hajmlardan va tezkor xotiradan ishonchli ma’lumotlarini kriminalistik aniqlik bilan xavfsiz olishni amalga oshiradi. Dastur agenti oson o‘rnatiladi. Noqulay o‘rnatish va autentifikatsiya qilish jarayonini talab qilinmaydi. Masofali qurilmalar xavfsiz o‘rnatiladi.

Ko‘p funksionallikka ega intuitiv interfeys. Moslashtirilgan ma’lumotlar formatlari, rivojlangan filtrlash, ko‘chiriladigan oyna va avtomatlashtirilgan ma’lumotlar tasnifiga ega osonlashtirilgan va oson ishlatiladigan grafik interfeys.

5.7. EnCase Forensic texnologiyasi yordamida kompyuter ekspertizasi

Hozirgi vaqtda va uzoq yillardan buyon Guidance Software kompyuter ekspertizasi uchun vositalarni ishlab chiqaruvchi yetakchilardan biri hisoblanadi. Ishlanmalarning sezilarli, katta qismi - kompyuter mutaxassislarini o‘qitish dasturlari va vositalari.

EnCaseForensic dasturiy vositalari va texnologiyalari yordamida har qanday bosqichda har xil turdagi tadqiqotlar o‘tkazish va aniq turli ekspert maslahatini berish imkoniyati bor.

Guidance Software firmasi mahsulotlari va EnCaseForensic maxsus texnologiyalari bilan sud tibbiyoti mutaxassislarini o‘qitish

mumkin. Barcha sertifikatlangan mutaxassislar va umuman barcha mutaxassislar butun dunyo bo‘ylab kompyuter ekspertizasi va axborot texnologiyalari sohasida faoliyat yurituvchi Guidance Software kompaniyasidan ekspert sertifikatini qo‘lga kiritislari mumkin.

Kompyuter ekspertizasining barcha bosqichlarini o‘tkazish uchun texnologiya va dasturlar to‘plami - EnCase o‘zi nima?

EnCase Forensic - bu raqamli dalillarni izlash va sudga ma’lumotlarni taqdim etish bo‘yicha xalqaro standart bo‘lgan kompyuter va texnik ekspertiza uchun lokal dasturiy ta’minotdir. EnCase Forensic mutaxassislar tomonidan tayyorlangan filtrlar va modullarning ko‘plab ma’lumotlarini olish, qattiq diskda mavjud bo‘lgan ma’lumotlarning sud-tahlilini o‘tkazish orqali potensial dalillarni aniqlash va olingan natijalarning ishonchliligi va yaxlitligini ta’minlashda natijalar haqida to‘liq hisobotlarni tayyorlash imkonini beradi.

Kompyuter-texnik ekspertizani o‘tkazish standartiga aylangan va vaqt o‘tishi bilan sinalgan mahsulot yordamida dalillarni izlash to‘griligining kafolatini beradi.

– qidirish mexanizmlarini keng ko‘lamli yordamida maslahatlar olish imkonini beradi.

– umumiy vazifalari avtomatlashtirish hisobiga tadqiq qilishni tezlashtiradi.

– EnCase bazasidagi yagona konteynerda dalillarni saqlaydi.

EnCase Forensic kriminalistik ekspertizasining barcha prinsiplariga va sudda foydalanish imkoniyatlariga muvofiq topilgan barcha dalillarni bitta faylda saqlaydi.

Kuchli va samarali kriminalistik ma’lumotlarni qidirish va kompyuter Insidentlarini o‘rganish natijasida EnCase Forensic korporativ tekshiruv va ma’lumotlar auditi bo‘yicha standart vositaga aylangan.

Ushbu ham dasturiy va ham apparat vosita - maxsus dasturlarga qo‘shimcha ravishda, FastBloc qurilmasidan foydalanib, manbalarga va saqlash vositalariga kirish uchun o‘z texnologiyasiga ega. EnCase dasturiy vositalari kabi, FastBloc ham MSWindows ishlaydi, uning muhitida natijalarni ko‘rsatadi. Va bu mutlaqo aniq - mutaxassis va huquqiy nuqtai nazardan - axborot tashuvchilariga va ulardagi axborotlarga kirishni ta’minlaydi, dastlabki ma’lumotlar tashuvchilari va ularning tarkibidagi ma’lumotlarni buzmasdan tadqiqotni va nusxa ko‘chirishni amalga oshiradi.

Ma’lumotlar original axborot vositalaridan, kompyuter ekspertizasi qoidalariga muvofiq, muayyan tarzda qayd qilingan barcha qadamlar bilan nusxa ko‘chirilib, dastlabki ma’lumotlarni ekspertiza qilish uchun olingan holda saqlaydi. EnCase texnologik vositalarining faoliyati Case-metodologiyaga asoslangan, u tadqiq qilish jarayonida va keyin tadqiq qilishning obyektlari bo‘lmish ma’lumot va uning tashuvchisini ilk holatdagidek saqlashga mas’uldir.

EnCase dasturiy ta’minotining texnologik imkoniyatlari va Case-metodologiyasi. EnCase va ularning metodologiyasi – tadqiq qilish uchun mo‘ljallangan boshqa vositalr bilan taqqoslaganda ekspertizaga ijodiy va ko‘p qirrali yondashishga ko‘proq mos keladi. Ko‘plab xorijiy ekspertlar allaqachon EnCasening chiqqan versiya majmualari bilan ishlash tajribasiga ega, ular o‘z vazifasini yangi ma’lumot tashuvchilarida, bugunda kompyuter ekspertizasi ko‘rib chiqishi kerak bo‘lgan yangi fayl turlari va vaziyatlari bilan muvaffaqiyatli choralar ko‘radi.

Ushbu texnologiyaning imkoniyatlarini yanada yaxshiroq tushunish uchun, ular tomonidan taklif qilinadigan vazifalarni ko‘rib chiqaymiz:

– EnCase bazasida chuqur sozlash va o‘z vositalarini yaratish imkoniyati. EnCase tizimiga joylangan ESCRIPT deb nomlanuvchi dasturlashning makrotili dasturni sozlovchi va imkoniyatlarini kengaytiruvchi dastur va filtrlarni yaratadi. Shu yo‘l bilan EnCaseda zamonaviy metodlarni zamonaviy sharoitlarda qo‘llashga yo‘l beradi;

– turli formatdagi media, eski va yangi formatlar, turli xil apparat platformalarida, operatsion tizimlar nuqtai nazaridan turli muhitlarda, statsionar va harakatlanuvchi media turlarining turli xil ko‘rinishlari bo‘yicha axborotni tahlil qilish va qidirish. Har xil turdagi qattiq va almashinuvchi drayvlar va boshqa tashuvchilar turlari;

– grafik tasvirlar bilan ishlashda grafik fayllarni tanib olish, ularni avtomatik ravishda belgilash va nusxalash uchun katta imkoniyatlar yaratadi;

– tashuvchi tarkibini ekspert o‘rganish uchun maxsus mo‘ljallangan stend disklariga aniqlik bilan to‘liq nusxasini ko‘chirish;

– qattiq diskning to‘liq nusxalari va uning tarkibi, mantiqiy birlik va bo‘limlar bilan ishlash uchun moslashuvchan operatsiyalar;

– RAID-massivlar va u bilan turli yo‘nalishda ishlash - qo‘llab quvvatlanadi;

– mutaxasis va kriminalistlar uchun tashuvchida mavjud ma’lumotlarni oldindan va tezda hamda o‘zgartirishlar kiritmay ko‘rib chiqish muhim hisoblanadi. Buning uchun EnCaseda maxsus texnologiyalar mavjud. Materiallar daxlsizligicha qolaveradi, ayni paytda ma’lumot tashuvchi vositalarni ba’zi mazmunli ma’lumotlarning mavjudligigatezda tekshirib ko‘rishingiz mumkin;

– FastBloc markasidagi apparat vositalari bilan istalgan turdagi qattiq disklarga har tomonlama xavfsiz va aniq kirishni ta’minlash mumkin.

Bu savol va vazifalarni hal qilish, tashuvchilar bilan ishlash, ularga kirish, ularni tahlil qilish, butun EnCase tizimini yanada samaraliroq ishlash uchun yaratish va EnCase- ni zamonaviy kompyuter mutaxassisliklarida ishlatish bilan bog‘liq. Kompyuter mutaxassisligi bo‘yicha alohida, mutaxassislarni albatta qiziqtiruvchi, bu turdagi murakkab kompleks ishining bo‘limi - bu uning fayl va fayllar tizimi bilan ishlash qobiliyatidir.

EnCase dasturidan foydalangan holda fayllar bilan xilma-xil ishlash va kompyuter ekspertizasi. Kompyuter ekspertizasi imkoniyatlari, turli yo‘nalishlarda, sud yoki suddan tashqari, hukmi ko‘pincha fayllar va fayl tizimlari bilan ishlash uchun foydalaniladigan dasturiy ta’minot tizimlari imkoniyatiga bog‘liq. Fayllarni sozlash va fayllar bilan ishlash qanchalik mos bo‘lishi mumkin, fayllar tuzilmasi, fayl turlari va tarkibini tahlil qilish qanchalik tez amalga oshirilishi mumkin - qo‘yilgan vazifalarni amalga oshirishda mutaxassislarning imkoniyatlari chegaralangan yoki chegaralanmagan bo‘lishi shularga bog‘liq.

Fayllar bilan ishlashga kelganda Guidance Softwarning EnCase dasturi quyidagi imkoniyatlarga ega, ularning bari tashuvchi holati va ilk olingan ma’lumotga putur yetkazmasdan amalga oshiriladi:

– har qanday fayllarning tarkibini, yaratilish, o‘zgartirish sanalari va boshqa attributlarni aniqlash;

– fayllarni ochmasdan, fayl tizimining strukturasini o‘zgartirish xavfsiz, himoya mexanizmlari va boshqa dasturlarni ishga tushirmasdan fayldagi kalit so‘zlar, izlanuvchi so‘zlar, matn, alifbo-raqamli ma’lumotlarini izlash;

– siqilgan, berkitilgan, arxivlangan, operatsion tizim ro‘yxatida qayd etilgan, maxsus va keng tarqalgan xususiyatli turli fayllar kabi fayllarni tezkorlik bilan izlash, nusxalash, ajratish, o‘rganish;

– e-pochta va xabarlarni boshqa yo‘llar bilan tarqatish usullari bilan ishlashda – qo‘shilgan va turli xil shakl, formatdagi fayllarni tahlil qilish;

– barcha ma’lumot va barcha fayllar tashuvchilarining nusxasini o‘rganish maqsadida grafik ko‘rinishda ko‘rsatish

Sektorlar va klasterlarning tuzilishini ko‘rsatish. Har qanday faylning joylashuvini grafik va axborot aks ettirish:

– belgi, tanlash, nusxa ko‘chirish, uzatish va eksport fayllar, fayl strukturasi va katalog daraxti, fayllar individual parchalar qismlari;

– turli fayllarni imzolar bilan ilmiy-tadqiqot ishlari, EnCase mavjud bo‘lgan fayl imzolari kutubxonasini kengaytirish va o‘zgartirish;

– ekspert ishlov va ma’lumotni avtomat ravishda tanishni qulaylashtirish uchun kutubxona qurilishi, fayllarning strukturasi, formati, tipiga ko‘ra maxsus joylashtirish;

– spooler-fayllar, slack-fayllar, swap--fayllar va hokazolar sirasiga kiruvchi fayllarning tarkibini o‘rganish imkoni. Shuningdek, o‘chirish, savatga ko‘chirish va hokazo;

– EnCase tizimida ish tugaganda vaqt va sanalar qo‘shilgan to‘liq hisobotni tuzishga yordam berishga mo‘ljallangan qulay vositalar ko‘zda tutilgan. Bu yuridik va mutaxassislik yuzasidan to‘g‘ri xulosalarni sud va boshqa maxsus instansiyalarga topshirish uchun katta qulayliklar beradi.

Interfeys. Ekspert uchun EnCase dasturiy vositalarining muhim va qulay xususiyatlari. Ushbu sohadagi ishlar bilan yaqindan tanish bo‘lmagan va uning turli xil nozik xususiyatlaridan bexabar bo‘lgan ekspertlar uchun ushbu ro‘yxatdagi turli punktlarda qanday imkoniyatlarning muhokama qilinganligini misollar bilan tushuntirish foydali bo‘lishi mumkin. Ushbu dasturning asosiy afzalliklaridan birini aniqlaymiz. Bizga ko‘rinib turibdiki, EnCase ning qulayligi, asosan, grafik interfeyslarning qulayligi - mediadan nusxalarning va har qanday fayllarning mazmunini va boshqa ma’lumotlarni ko‘rsatish turlari bilan bog‘liq.

«EnCase" to‘plamidan foydalanib, "ijodiy" tadqiqot o‘tkazish qobiliyati haqida gapirganda, dasturni makrotilidan foydalanib uni ichki

sozlashni, turli turli operatsiya va holatlar uchun operativ interfeys nuqtai nazaridan dastur va ma’lumotlar, jumladan tashqaridan qabul qilinuvchi axborot bilan ishlashni o‘zgartirishni tushunamiz. Bundan tashqari, zamonaviy mutaxassislar uchun ma’lumot "foydalanuvchi interfeysi" ning qulay ko‘rinishida taqdim etilishi muqobilroq. Misol uchun, EnCase interfeysi quyidagi xususiyatlarga ega: CaseTab tanlovi yordamida standart Windows Explorer kuzatuvchisidagidek fayllarni namoyish qilishingiz mumkin. Chapda papka va fayllar daraxtini olsangiz, o‘ng tomonda Report, Timeline, Gallery, Table (hisobot, xronologiya, galereya, stol) singari qo‘shilmalar haqida ma’lumot mavjud. View File Structure buyrug‘i yordamida arxivlangan va siqilgan fayllarning mazmunini "ma’lumotlarga tegmasdan"ko‘rish juda oddiy.

Turli xususiyatlar va atributlarga tayangan holda, fayllarni tashkil qilish va va ularni TableView funksiyasi yordamida qulay grafik interfeys ko‘rinishida jadval orqali dastur oynasining yuqori qismida namoyish qilish mumkin. Bundan tashqari, u oynaning pastki qismida mazmuni jihatdan jismoniy disk ko‘rinishini ham nazarda tutadi.

KeywordsTab dan foydalanib, qiziqtiradigan kalit so‘zlar, ularning toifalari va qidiruvi bilan juda qulay ishlash mumkin. Kerakli ma’lumotlarni kodlashni tanlash, keyingi ishlar uchun yangi kalit so‘zlar kategoriyalarini yaratish imkoni mavjud.

Qo‘shilma jadvali Bookmarks Tab barcha topilgan mosliklar uchun qo‘shilmalar jadvali ko‘rinishini taklif qiladi. Havolalar turli papkalarda taqsimlanishi, qo‘shilmalar turli xil shakllarda tashkil qilinishi va ularning turli ko‘rinishi belgilanishi mumkin: Report, Timeline, Gallery, va Table. Ushbu usullar turli xil fayllarni namoyish qilish, ularning vaqt oralig‘ini ko‘rish uchun mo‘ljallangan - sizni qiziqtirgan vaqtlarni sozlash qobiliyati ham mavjud.

Asosiy xulosalar

Topilgan ma’lumotlar tufayli o‘tkazilgan kriminalistik tadqiq qilish dallil sifatida xizmat qilishi mumkin.

Har xil tashuvchi vositalarda saqlangan, o‘chirilgan yoki shikastlangan ma’lumotlarni qayta tiklash quyidagilarni qayta tiklash orqali amalga oshiriladi: turli xil o‘chirilgan fayllar; kompyuter viruslari ishidan keyingi ma’lumotlar; fayl tizimlarining mantiqiy shikastlanishidan keyingi ma’lumotlar; nosoz kompyuterda saqlangan ma’lumotlar; dastur xatoligi tufayli zararlangan fayllar.

Kriminalistik ahamiyatli ma’lumotlarni yuborish va olishni nafaqat statsionar kompyuter vositalari va tizimlari, balki mobil aloqa telefonlari, smartfonlar, planshet kompyuterlari uchun ham ko‘rib chiqish kerak, negaki ular faqatgina ahamiyatli ma’lumot tashuvchi yoki uzatuvchisi bo‘lib qolmay, balki jinoyat sodir etish predmeti va quroli bo‘lishi ham mumkin.

Quyidagi ekspertiza turlari mavjud:

- apparat - kompyuter ekspertizasi;
- dasturiy - kompyuter ekspertizasi;
- axborot - kompyuter ekspertizasi;
- kompyuter - tarmoq ekspertizasi;
- kompleks ekspertiza.

Texnik tizimlarni apparat ekspertizasidan o‘tkazish jinoyat sodir etilganligi to‘g‘risidagi axborotni saqlovchilarning to‘g‘ri ishlashini o‘rganishga qaratilgan.

Dasturiy - kompyuter ekspertizasi jinoiy yoki fuqarolik ishlarida haqiqatni aniqlash uchun mo‘ljallangan kompyuter dasturlarini ishlab chiqish va qo‘llash qonunlarini o‘rganadi.

Axborot-kompyuter ekspertizasi kompyuter ma’lumotlariga oid diagnostika va identifikatsiyalashning ko‘plab muammolarini yakuniy hal etish orqali dalil bazasini yaxlitlashni yakunlash imkonini beradi.

Kompyuter-tarmoq ekspertizasi har qanday tarmoq axborot texnologiyasini amalga oshiradigan kompyuter vositalarining funksional maqsadlariga asoslangan.

Ichki kompyuter tekshiruvini muvaffaqiyatli o‘tkazish uchun Insidentga tezkor javob beruvchi guruhni tuzish kerak.

Raqamli kriminalistikada qo‘llaniladigan tan olingan dasturiy vositalar to‘plami (FTK) tezkor, barqaror va qulay foydalanish uchun mo‘ljallangan sud tomonidan tan olingan dastur bo‘lib, u kriminalistik aniqlik bilan ma’lumotlarni tahlil qiladi, parollarni deshifrlaydi va buzadi.

Kompyuter ekspertizasining barcha bosqichlarini amalga oshiruvchi texnologiyalar va dasturlar (EnCase Forensic) ekspertlarga tayyor filtr va modullarning keng ko‘lami yordamida ma’lumot olishga, qattiq diskdagi axborotning kriminalistik tahlili asosida potensial dalillarni topishga, olingan natijalar bo‘yicha hisobot tayyorlashga, shu bilan birga, olingan dalillarning yaxlitligi va ishonchliligini ta’minlashga imkon beradi.

Nazorat uchun savollar

1. Kompyuter axboroti va hisoblash texnikasi vositalarini kriminalistik tadqiq qilish nimaga asoslangan?

2. Ma'lumotlar qanday tiklandi?

3. Sud kriminalistika ekspertizaning asosiy prinsiplari.

4. Raqamli ko'rinishda saqlanuvchi dalillarning o'ziga xos xususiyatlarini sanab o'ting.

5. Kompyuter -texnik ekspertizaning mohiyati.

6. Texnik tizimlarni apparat ekspertizasining asosiy vazifalari.

7. Kompyuter mutaxassisi qanday muammolarni hal qilishi kerak?

8. Sud ekspertlari uchun qanday vositalar mavjud?

9. O'rganish turi, kategoriyalari va vazifalarini sanab o'ting

10. Tadqiq qilish jarayonida qanday bosqichlar mavjud?

11. Raqamli dalillarni to'plash jarayoni qanday amalga oshiriladi?

12. Forensic Toolkit raqamli sud-tibbiyot ekspertizasi qanday vazifalarni hal qiladi?

13. *EnCase Forensic kompyuter ekspertizasini o'tkazish uchun texnologiyasi va dasturi qanday imkoniyatlarni taqdim etadi?*

6. KIBER JINOYATCHILIK MUAMMOLARI

6.1. Zamonaviy kiber jinoyatchilik

2015-yilda 2,5 milliard odam yoki sayyoramiz aholisining uchdan bir qismidan ko‘pi Internetga kirish imkoniga ega edi. Internetdan foydalanuvchilarning 60 foizdan ortig‘i rivojlanayotgan mamlakatlarda yashamoqda va Internetdan foydalanuvchilarning 45 foizini 25 yoshgacha bo‘lganlar tashkil qiladi. Hisob-ktiobga ko‘ra, 2019 yilga borib, jahon aholisining 70 foizigacha mobil kengmiqyosli internetdan foydalanish imkonini qo‘lga kiritadilar. 2020 yilga borib, tarmoq qurilmalari soni («Internet buyumlar») aholi sonidan olti barobar ortadi, bu Internetning joriy tushunchasini butunlay o‘zgartiradi.

Tarmoqqa o‘ta ravishda ulangan kelajak dunyosida internet-protokolga (IP) ulanish bilan bog‘liq elektron dalillar bilan birga uchramaydigan “kompyuter jinoyati” va balki umuman har qanday jinoyatni tasavvur qilish qiyin.

Kiber jinoyatning ta’rifi ushbu termini qanday maqsadda ishlatilishi bilan belgilanadi.

Tor ma’nodagi kiber jinoyat (kompyuter jinoyati) - bu kompyuter tizimi va u qayta ishlovchi ma’lumotlarga nisbatan yo‘naltirilgan elektron operatsiyalar ko‘rinishidagi har qanday noqonuniy harakat. **Keng ma’nodagi kiber jinoyat** (kompyuterlarni qo‘llash bilan bog‘liq jinoyat) - bu kompyuter tizimi yoki tarmoq yordamida yoki ular bilan birgalikda amalga oshiriluvchi har qanday noqonuniy harakat, jumladan, kompyuter tizimi yoki tarmoq yordamida ma’lumotning noqonuniy qo‘lga olinishi, taklif qilinishi yoki tarqatilishi.

Kiber jinoyatning asosi kompyuter ma’lumotlarining yoki tizimlarining maxfiyligi, yaxlitligi va mavjudligiga nisbatan cheklangan qator tadbirlar hisoblanadi. Ammo bu bilan cheklanmasdan, kompyuterdan shaxsiy yoki moliyaviy foyda ko‘rish, shaxsiy yoki moliyaviy zarar yetkazish maqsadida kompyuterdan foydalanishni, jumladan, shaxsiy ma’lumotlarni ishlatish, kompyuter ma’lumotlari tarkibi bilan bog‘liq kirdikorlarni (ularning bari “kiberjinoyat”ning keng tushunchasiga kiradi) qo‘shsak, barchasini qoplovchi huquqiy ta’rifini topish qiyinlashadi. Kiber jinoyatlarning asosini tashkil etuvchi jinoyatlar uchun ba’zi ta’riflar kerak. Biroq kiber jinoyatchilik “ta’rifini” aniqlash biron bir jinoyatni sodir etishning elektron dalillarini topish bilan ko‘proq bog‘liq bo‘lgan

qator maxsus tergov vakolatlarini va xalqaro hamkorlik imkoniyatlarini aniqlash kabi boshqa maqsadlardan juda muhim emas. Shu sababli “kiberjinoyat” tushunchasiga harakat va faoliyatlar birlashmasi deb qarash maqsadga muvofiq.

Ijtimoiy-iqtisodiy manfaatlardan tashqari, kompyuter texnologiyalari va Internet ham, odamlar o‘rtasidagi o‘zaro munosabatlarning imkoniyatlarini kengaytiruvchi boshqa vositalar kabi, jinoyatlarni sodir etishda ishlatilishi mumkin. Kompyuter yordamida amalga oshiriluvchi jinoyatlar yoki kompyuter jinoyatlar nisbatan uzoq vaqtdan beri davom etayotgan hodisani tashkil etsa-da, global tarmoqqa ulanishning o‘sib borishi zamonaviy kiber jinoyatlarning rivojlanishi bilan uzviy bog‘liqdir.

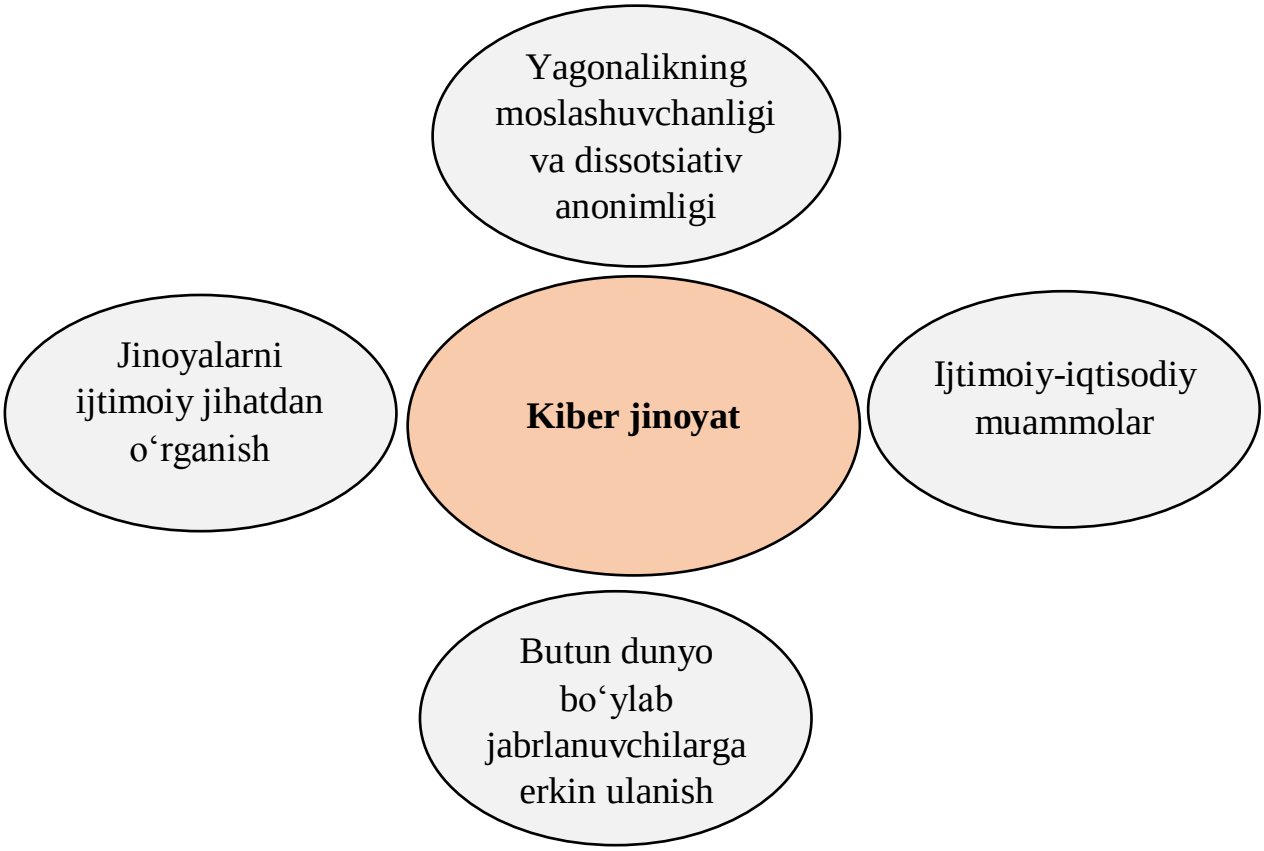
Zamonaviy kiber jinoyatchilikning asosi - global axborot-kommunikatsiya texnologiyalarining yaqinlashuvi transmilliy miqyosda jinoyatlarni sodir etish uchun ishlatilishi mumkin degan fikrdir.

Bunday jinoyatlar yuqorida ko‘rsatilgan barcha kompyuter jinoyatlarini, shuningdek, kompyuter yoki Internet-kontent bilan bog‘liq, shaxsiy yoki moliyaviy daromad uchun kompyuterdan foydalanish kabi ko‘plab boshqa jinoyatlarni o‘z ichiga olishi mumkin.

Shunga qaramay, bugungi kundagi va ayniqsa ertangi kiber jinoyatchilikning markaziy elementi sifatida global tarmoqqa ulanish ko‘rilishi kerak. Kibermakon va IP-trafikning kengayishi hamda simli ulangan qurilmalarga nisbatan simsiz ulangan qurilmalarning trafigi ortishi, kompyuter bo‘lmagan qurilmalar internet-trafigining ko‘payishi bilan bir qatorda, global tarmoqqa IP-ulanishsiz ro‘y bergan kompyuter jinoyatlarini tasavvur qilish qiyin. Mobil qurilmalarning maxsus moslashtirilganligi va maishiy texnika yoki shaxsiy buyumlarning internet-prorokollariga ulanishi elektron ma’lumot va ularning uzatilishi deyarli har bir inson xatti-harakatlarining, u qonuniy yoki noqonuniy bo‘lsin, ajralmas qismi bo‘lishiga olib keladi.

Kiber jinoyatlar o‘sishining asosiy sabablari. Kriminologiya nuqtai nazaridan, axborot-kommunikatsiya tizimlari va Internetdan foydalanishning ko‘payishi jinoyatchilar uchun yangi imkoniyatlar yaratilishiga va jinoyatlar o‘sishini rag‘batlantirishga sabab bo‘lishi mumkin (24- rasm).

Garchi bu holatda bir qator kriminologik nazariyalar qo‘llanilishi mumkin bo‘lsa-da, kiber jinoyat "yangi va turli xil jinoyat turi" bo‘lishi jinoyatchilikning umumiy nazariyasini qo‘llash orqali o‘zgaruvchan vaziyatni oldindan ko‘ra bilishda va bunday jinoyatlarning oldini olishda muammolarni keltirib chiqaradi.



24- rasm. Kiber jinoyatlar sodir etilishining ehtimolli sabablari

Asosiy taxminlardan biri “kiberjamiyatning” rivojlanishi kompyuter tizimlarining mavjudligi, kompyuterlar taqdim etuvchi bevosita jinoyat imkoni bilan bog‘liq bo‘lmagan yangi fenomenlarning shakllanishiga olib keladi. Inson jismoniy dunyoga nisbatan kibernetika ichida qonuniy va noqonuniy xatti-harakatlar o‘rtasidagi farqni ko‘rsatishi mumkin. Masalan, kiber makonda odamlar jismoniy dunyoda o‘z maqomlari va pozitsiyasi tufayli sodir bo‘lmagan jinoyatlarni sodir etishlari mumkin. Bundan tashqari, identifikatsiyalash moslashuvchanligi, dissotsiyativ anonimlik va cheklovlar yo‘qligi kibernetika sohasidagi jinoyatiy xatti-harakatlarni rag‘batlantirishi mumkin.

Odatiy ishlarning konsepsiyasi ham kiber jinoyatlarning asosiy kuchlarini aniqlashga yordam beradi. Kundalik faoliyat konsepsiyasi

jinoyatchilik xavfi o‘zaro aloqa bilan ortib borayotganligini ko‘rsatadi: manfaatdor jinoyatchi, mos qurbon va samarali advokatning yo‘qligi. Kiber jinoyat holatida ko‘plab mos keluvchi qurbonlar global tarmoq o‘tkazilayotgan vaqtining va bank, xarid qilish va fayllarni almashish kabi onlayn xizmatlardan foydalanishning ko‘payishi tufayli foydalanuvchilarning fishing yoki firibgarlik qurbonlari bo‘lish xavfini yuzaga keltirishi mumkin.

Shu jumladan, «Twitter» va «Facebook» singari ijtimoiy tarmoqlarning rivojlanishi millionlab potensial firibgarliklar yoki qurbonlar shakllanishiga sabab bo‘ladi. Agar foydalanuvchilar faqatgina "do‘stlar" doirasidan tashqaridagi muloqotni cheklovchi sozlamalarni ishlatmasalar, bunday ijtimoiy tarmoqlar ularni darhol ko‘plab potensial qurbonlarga ulanish imkonini beradi. Bundan tashqari, odatda ijtimoiy tarmoqlardagi profillarini o‘zining qiziqishlari va joylashuvi asosida joylashtirishi jinoyatchilarga muayyan xatti-harakat yoki biografik ma’lumotlar bilan birlashtirilgan qurbonlarga hujum qilish imkonini beradi. Mavjud “himoya” choralari, masalan, antivirus dasturlari va jinoyatni to‘g‘rilash tadbirlari (nisbatan katta bo‘lmagan) yirik foyda ko‘rishni maqsad qilgan qonunbuzarni to‘xtashish uchun yetarli bo‘lmasligi mumkin.

Tashkillangan guruhlar tomonidan sodir etiladigan kiber jinoyatlarning asosiy sabablariga global tarmoqqa ulanish va o‘ziga o‘xshashlar bilan ma’lumot almashinish kiradi. Bundaylarga yana bir misol, “karding” yoki o‘g‘rilangan ma’lumotlarni almashish uchun kredit kartalari ma’lumotlarini o‘g‘irlovchi firibgarlardir. Kredit kartalar to‘g‘risidagi ma’lumotlarni o‘g‘rilovchi firibgarlar forumlari ko‘pincha “tartibsiz” strukturada boshqaruv zanjirisiz shaklda hosil bo‘ladi, bunda firibgarlar bilimlarni almashish va xizmatlarni taklif qilish uchun bir-birini izlashadi vaglobal tarmoqda “uchrashishadi”. Keyinchalik, forumlar yanada yuqori darajadagi tashkilotga ega "markaz" vazifasini bajaradigan ko‘proq nazorat qilinadigan jinoiy guruhlarga aylantirildi. Ijtimoiy tarmoqlar ijtimoiy-targ‘ibot va shaxsiy jinoyatchilar va jinoyatchi guruhlar o‘rtasidagi muloqot uchun ham ishlatilishi mumkin.

Ijtimoiy-iqtisodiy omillar ham kiber jinoyatlarning o‘sishini rag‘batlantirishda muhim rol o‘ynashi mumkin. Xususiy sektor korxonalari harajatlarni kamaytirishga va xodimlar sonini qisqartirishga majbur bo‘ladigan holat, masalan, xavfsizlikning kamayishi, axborot va aloqa tizimlarida zaif nuqtalardan foydalanishga olib kelishi mumkin. Kompaniyalarning chetki xodimlar yoki vaqtinchalik pudratchilarni

yollashi yoki kompaniyalar ishchilari o‘rtasida ish haqining pastligi va ish joyini yo‘qotishdan qo‘rqqani sababli noroziliklari mavjudligi sababli kompaniyalarning muayyan "ichki a’zolari" yoki jinoiy guruhlarning ularga ta’siri xavfli bo‘lishi mumkin. Kiber xavfsizlik bilan shug‘ullanuvchi ba’zi kompaniyalar shtat qisqarishiga duchor bo‘lgan xodimlar iqtisodiy pasayish davrida sodir bo‘lishi mumkin bo‘lgan xavflarni tug‘dirishidan xavotirlanadilar. Shuningdek, uyushgan jinoyatchilik uchun yangi manbaga aylanishi mumkin bo‘lgan, oliy ma’lumotga va kompyuterga ega bo‘lgan ishsiz yoki yarim kunlik talabalar soni ortib bormoqda.

6.2. Kiber jinoyatchilikning klassifikatsiyasi

Xalqaro elektraloqa ittifoqi (MSE) kiber jinoyatchilikning quyidagi batafsil klassifikatsiyasiini taklif qiladi:

1. Kompyuter ma’lumotlarining yoki tizimlarining maxfiyligi, yaxlitligi va mavjudligiga qarshi jinoyatlar

- kompyuter tizimlariga noqonuniy kirish (xakerlik, shifrni buzish);
- kompyuter ma’lumotlariga noqonuniy kirish, ularni qo‘lga olish yoki tutish (axborot josusligi);
- ma’lumot yoki tizimga noqonuniy aralashuv;
- kompyuterdan qonuniy foydalanish vositalarini ishlab chiqarish, tarqatish va saqlash;
- ma’lumotlar himoyasi choralarini yoki maxfiyligini buzish.

2. Kompyuterdan foydalanish bilan bog‘liq jinoyatlar

- kompyuter firibgarligi yoki qalbakilashtirish;
- shaxsiy ma’lumotlar bilan bog‘liq kompyuter jinoyatchiligi;
- mualliflik huquqi yoki tovar belgilari bilan bog‘liq kompyuter jinoyatchiligi;
- spamni tarqatish yoki tarqatishni nazorat qilish;
- shaxsiy jabr maqsadida kompyuterdan foydalanish harakatlari;
- bolalarni jalb qilish va gruming maqsadida kompyuterni qo‘llashni nazarda tutuvchi harakatlar.

3. Mazmun bilan bog‘liq jinoyatlar

- nafratni targ‘ib qilish bilan bog‘liq jinoyatlar;
- bolalar pornografiyasini ishlab chiqish, tarqatish va saqlash uchun kompyuterdan foydalanish;
- jinoyatda hamkorlik uchun kompyuterdan foydalanishni nazarda tutuvchi harakatlar;

- diniy jinoyatlar;
- tuhmat va qalbaki ma’lumotlar;
- spam va u bilan bog‘liq jinoyatlar.

4-ilovada ushbu harakatlarning har birining batafsil tavsifi keltirilgan. Maqsad “kiber jinoyatchilik” atamasiga kiritilishi mumkin bo‘lgan taxminiy harakatlar ro‘yxatini tuzishdir.

Shu bilan bir qatorda, shuni ta’kidlash kerakki, internet va shaxsiy kompyuterlarning keng tarqalishi komyuter yoki tizim ma’lumotlari har qanday turdagi jinoyatlarni sodir etish uchun qo‘llanilishi mumkin. Shuning uchun konsepsiya jihatdan farqlansada, elektron dalillar sohasi kiber jinoyatchilik bilan bog‘liq. Elektron dalillarni to‘plash va taqdim etish kiber jinoyatni tergov qilish va sud tomonidan taftish etilishining ajralmas qismidir. Bundan tashqari, bu borgan sari odatiy jinoyatlar, jumladan kissavurlik, o‘g‘rilik yoki o‘g‘rilik va buzish hamda turli xil tashkiliy jinoyatlarga tegishli bo‘lmoqda. Telefon orqali suhbatlar, elektron pochta, aloqa jurnallari, SMS-xabarlar, mobil telefonlarning manzillari va kompyuter fayllarini kompyuter yozuvlari deyarli har qanday turdagi jinoyatda shubhalanuvchining joylashuvi, maqsadi, jinoyat sodir etilgan hududda bo‘lganligi yoki unga jalb qilinganligi yuzasidan dalillarni saqlashi mumkin.

14 jinoyat turidan iborat ro‘yxat to‘liq deb hisoblanilmaydi. Kiber jinoyat deb qaralishi mumkin bo‘lgan boshqa qilmishlar: “moliyaviy vositalar va to‘lov vositalari bilan bog‘liq noqonuniy ishlarni amalga oshirish maqsadida kompyuter vositalaridan foydalanish”, “onlayn rejimda qimor o‘yinlari”, “odam savdosi maqsadida axborot texnologiyalari birliklarini qo‘llash”, “kompyuter yordamida giyohvand moddalar savdosi bilan noqonuniy shug‘ullanish”, “kompyuter yordamida talon-taroj qilish”, “parollarni noqonuniy tarqatish” va “maxfiy axborotdan foydalanish”.

Ba’zi hollarda qilmishlarga yuqorida sanab o‘tilgan kiber jinoyatlarning maxus shakli yoki variant deb qaralishi mumkin. Masalan, moliyaviy jinoyatni sodir etish uchun kompyuterni talab qiluvchi vosita sifatida foydalanish kompyuter firibgarligi yoki qalbakilashtirishning keng tushunchasiga kiritilishi mumkin. Maxfiy ma’lumotlarga kirish kompyuter ma’lumotlariga noqonuniy kirish turlaridan biri deb hisoblanishi mumkin. Parollarni noqonuniy tarqatilishi kompyuterlarni noto‘g‘ri ishlatish vositalaridagi ayrim qoidalarni qamrab olgan.

Internetga dunyo bo‘ylab har yerda kirish uchun sharoitlar yaratilar ekan, kiber jinoyat tushunchasini turli bosqichlarda qo‘llash ehtiyoji

tug‘ilishi mumkin: alohida kiber jinoyatlarni aniqlashda tushunchaning aniq va to‘liq tasviri zarur, bundan tashqari to‘xtovsiz real hayotdan global tarmoqqa ko‘chuvchi jinoyatlarga nisbatan butunjahon hamkorligining tergov o‘tkazish huquqlari va mexanizmlarini qo‘llash uchun samarali himoya mexanizmlari mavjud holatda keng yondashuv talab etiladi.

Kriminallashtirish. Tahlil qilish maqsadida tuzilgan savolnoma yordamida kiber jinoyat sohasidagi jinoiy qonunchilik ma’lumotlariga asosan hamda mamlakatlar qonunchiligi to‘g‘risida mavjud bo‘lgan hozirgi ma’lumotlarni qo‘llagan holda asosiy manbalarni o‘rganish orqali odatda kiber jinoyatchilik tushunchasi tarkibidagi 14 ta jinoyat belgilandi. So‘rovda ishtirok etgan davlatlar shuni ko‘rsatdiki, ushbu 14 jinoyat keng miqyosda kriminallashtiriladi, yaqqol istisno sifatida spam bilan bog‘liq jinoyatlar, bir qancha darajada kompyuterdan noqonuniy foydalanish bilan, millatchilik va irqchilik bilan, internetdan bolalarni jalb qilish va “gruming” uchun foydalanish qayd etildi. Davlatlar so‘rovnomada keltirilmagan ba’zi jinoyat turlarini keltirishdi. Ular asosan kompyuterda saqlanuvchi ma’lumotlarga tegishli edi, xususan, nomaqbul materiallar, onlayn qimorbozlik va giyohvandlik va odam savdosi bozori singari noqonuniy onlayn bozorlar shularning jumlasidandir. Ko‘rsatilgan 14 ta jinoyatga to‘xtalganda esa, davlatlar shuni xabar berishdiki, maxfiylik, ma’lumotlar yaxlitligi, kompyuter tizimlarining keng tarqalganligiga nisbatan asosiy kiber jinoyatlar uchun kiber jinoyatchilik sohasidagi maxsus jinoyatlar qo‘llaniladi. Kiber jinoyatning boshqa turlariga nisbatan kiber jinoyatchilikka bog‘liq bo‘lmagan umumiy turdagi qonunbuzarliklar qo‘llaniladi. Shu bilan birga, kompyuterdan shaxsiy hayotga aralashish, firibgarlik yoki qalbakilashtirish, shaxsiy ma’lumotlar bilan bog‘liq jinoyatlarni sodir etishda foydalanilganda ikkala yondashuv qo‘llaniladi.

Kompyuter tizimlari va ma’lumotlariga noqonuniy kirish jinoyat obyekti (axborot, tizim ma’lumotlari) va “shunchaki” kirish yoki yo‘qotish , zarar yetkazishning qo‘shimcha niyatlari bilan amalga oshirilgan ishning kriminalizatsiyasiga qarab farqlanadi. Kompyuter tizimlari yoki ma’lumotlari faoliyatiga aralashuv kriminallashtirilganda niyatning mavjudligiga yondashuv turlicha bo‘ladi. Ko‘plab mamlakatlarda aralashuv atayin uyushtirilgan bo‘lishi lozim bo‘lsa, boshqalarida ehtiyotsizlik tufayli yuzaga kelgan kirish ham hisobga olinadi. Kompyuter ma’lumotlariga aralashuv, o‘chirish va zarar yetkazishdan tortib to o‘zgartirish, bloklash, kiritish va tarqatishgacha

bo‘lgan qilmishlarni qamrab oladi. Ma’lumotning noqonuniy qo‘lga olinishining kriminallashuvi omma uchun mo‘ljallanmagan ma’lumotning qo‘lga olinishi bilan cheklangan yoki cheklanmaganligi, hamda ma’lumot “texnik vositalar” yordamida qo‘lga olinganligiga binoan farqlanadi. Barcha davlatlarda ham kompyuterning noqonuniy qo‘llanishi vositalari kriminallashtirilmaydi. Bu kriminallashtiriladigan davlatlarda jarayon jinoyatning kompyuter dasturlari va kirish kodlarini saqlash, tarqatish yoki foydalanishiga qarab bir-biridan ajraladi. Butunjahon hamkorligi nuqtai nazariga ko‘ra, bunday farqlanish ikki karra jinoiy javobgarlikka ta’sir qilishi mumkin.

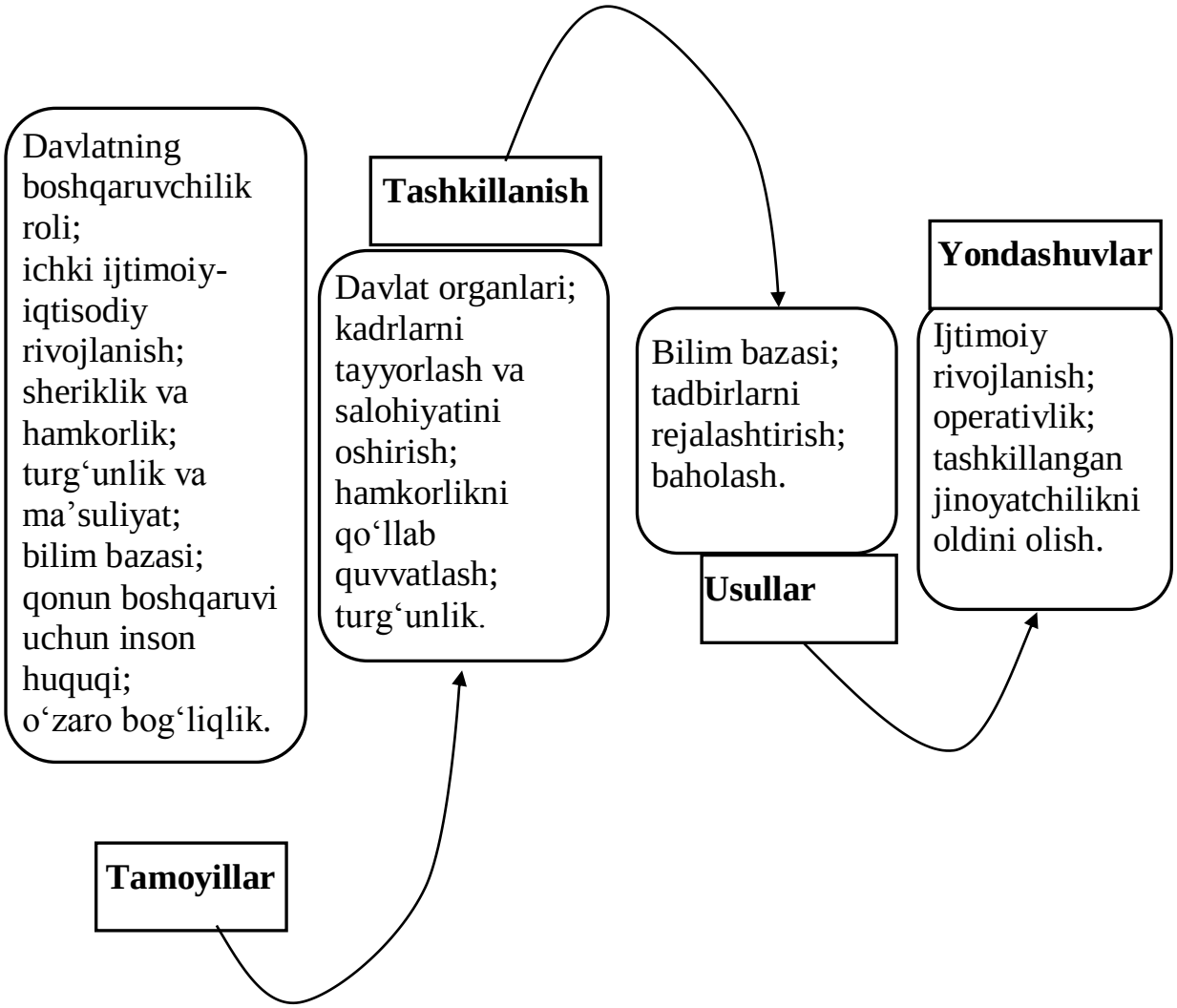
Qator mamlakatlarda maxsus kiber jinoyatlarga: kompyuter firibgarligi, qalbakilashtirish va shaxsiy ma’lumotlardan foydalanishga nisbatan munosabat qabul qilingan. Boshqa davlatlarda firibgarlik va o‘g‘rilikka nisbatan umumiy munosabat belgilanadi yoki asos tariqasida qilmishning markaziy elementini aks ettiruvchi jinoyat, jumladan, shaxsiy ma’lumotlarga bog‘liq holatda noqonuniy kirish, ma’lumotlarga aralashish va qalbakilashtirish olinadi. Ma’lumotlarning mazmuni, xususan, bolalar pornografiyasiga aloqador jinoyatlar kriminallashuvi juda keng tarqalgan. Biroq "bola" atamasi ta’rifida, vizual materiallarga nisbatan cheklovlar yoki simulyatsiya qilingan materiallar yo‘qligi hamda harakatlarga nisbatan ham nomuvofiqliklar mavjud. Garchi ko‘pchilik davlatlar bolalar pornografiyasini ishlab chiqarish va tarqatish qilmishlarini jinoyat deb hisoblasa-da, saqlash va foydalanishning kriminallashuvida sohasidagi keng qamrovli o‘zgarishlar kuzatilmoqda. Kompyuter jinoyatlariga kelsak, mamlakatlar ko‘pincha mualliflik huquqi va tovar belgilari bilan bog‘liq bo‘lgan qilmishlar ular qasddan va tijoriy maqsadda qilinsa umumiy jinoiy javobgarlikka tortilishini xabar qiladilar.

Ijtimoiy tarmoqlar va foydalanuvchilar tomonidan yaratilgan Internet kontentining ortib borayotgan ommaviyligi ko‘plab mamlakatlarda jazo qonunchiligi ko‘rilishiga olib keldi, bu esa so‘z erkinligi huquqlarini hurmat qilishga chaqirgan tartibga solish choralarini ko‘rishga sabab bo‘ldi. Respondent davlatlar so‘z erkinligini cheklashning turli darajalari, jumladan, ifloslanish, hurmatsizlik, tahdidlar, nafratni qo‘zg‘atish, diniy his-tuyg‘ularni haqorat qilish, odobsiz materiallarni tarqatish va jamoatchilikning xavotirlanishiga barham berish haqida hisobot beradi. Ba’zi cheklovlarning ijtimoiy-madaniy elementi nafaqat milliy qonunchilikda, balki ko‘p tomonlama hujjatlarda ham namoyon bo‘ladi. Bu borada, kiber jinoyatlarga qarshi

kurash bo‘yicha mintaqaviy hujjatlarda jamoat axloqi, pornografik materiallar va diniy, oilaviy prinsiplar yoki qadriyatlarning buzilishi bilan bog‘liq umumiy jinoyatlarni ko‘zda tutilgan.

6.3. Kiber jinoyatlarning oldini olish

"Jinoyatchilikning oldini olish" atamasi jinoyatchilik xavfini kamaytirishga qaratilgan strategiyalar va tadbirlarni va jinoyatchining ko‘plab sabablarini bartaraf etish bo‘yicha chora-tadbirlar orqali shaxslar va jamiyat uchun mumkin bo‘lgan zararli oqibatlarni qamrab oladi. Jinoyatchilikni oldini olish bo‘yicha ko‘rsatmalar jinoyatchilikning oldini olishda davlat organlarining boshqaruvchi funksiyalari vazirliklar va idoralar, shuningdek, davlat organlari va jamoat tashkilotlari, nohukumat tashkilotlari, biznes va jismoniy shaxslar o‘rtasida hamkorlik va sheriklik munosabatlarida muhim rol o‘ynashini ta’kidlaydi (25- rasm).



25- rasm. Jinoyatchilikning oldini olish tamoyillari, tashkiloti, usullari va yondashuvlari

Jinoyatchilik oldini olishning samarali yo‘li asosiy prinsiplarga (masalan, yetakchilik, hamkorlik va qonun ustuvorligi), tashkilot shakllarini (masalan, jinoyatlarning oldini olish bo‘yicha harakatlar rejalari) va metodlarni (masalan, mustahkam ma’lumot bazasini yaratish) va yondoshuvlarni (jumladan, jinoyatchilik imkoniyatlari va jinoyat qurbonlarini himoya qilishni kuchaytirish) asoslangan.

Kiber jinoyatlarning oldini olishda bir qator muammolar mavjud. Bunga ko‘plab potensial jabrdiydalarni taqdim etadigan Internet qurilmalarining mavjudligi va tarqalganligi; jismoniy shaxslarning global tarmoqda o‘zini “qaltis” ko‘rsatishga istagining nisbatan yuqori darajadaligi; huquqbuzar shaxslar tomonidan anonimligi va qo‘rqitishining ehtimoli; ko‘plab kiber jinoyatlarning transmilliy xarakteri; va jinoyatchilik yangiliklarining yuqori darajasi kiradi. Ushbu muammolarning har biri kiber jinoyatlarning oldini olish sohasidagi tashkilot, *usul* va *yondashuvlarga* ta’sir qiladi.

Shunday qilib, *tashkiliy* tuzilmalar kiber jinoyatchilikning oldini olish bo‘yicha xalqaro va mintaqaviy darajada hamkorlik qilish zarurligini aks ettirishi kerak. *Uslublar* kiber-faktlar tahdidining doimiy yangilanib turishini ta’minlashi kerak va *yondashuvlar* bir qator manfaatdor tomonlarning, xususan, Internet-infratuzilmasi va xizmatlarni boshqaradigan xususiy sektor tashkilotlarining ishtirokini o‘z ichiga olishi kerak.

Axborot xavfsizligi sohasidagi xavflarga ta’sir qiluvchi hozirgi davrning ikki o‘zgarishiga bulutli hisoblash xizmatlaridan foydalanishning ortishi va xodimlar tomonidan o‘zlarining raqamli vositalaridan (ayniqsa smartfon va planshetlar) foydalanish kiradi.

Oxirgi paytlarda xavfsizlik masalalariga bulutli hisoblashlarning ta’siri oshayotgani sezilmoqda. Masalan, texnologiya masalalari bo‘yicha kompaniya-konsultantlardan biri shuni ta’kidladi: ”Kichik kompaniyalar uchun kiber jinoyatchilik nuqtai nazaridan bulutli texnologiyalardan foydalanish buni server yordamida yerto‘lada amalga oshirishdan xavfsizroqdir. Kiber xavfsizlik bo‘yicha ekspertlarning soni har bir kompaniyani ta’minlash uchun yetarli emas va aniqki bu qimmatga tushadi. Shuning uchun himoya va javob berish nuqtai nazaridan, bunday resurslarni “Amazon”ga jamlash maqbulroqdir. Ammo bu hujum jabrdiydalarining paydo bo‘lishiga olib kelish ehtimoli bor, chunki kichik mahalliy magazin himoyasidan ko‘ra, yirik xizmat ko‘rsatuvchini buzish manfaatliroq”.

Boshqa muammo xodimlarning shaxsiy vositalaridan foydalanishidir. Texnologiya bo‘yicha kompaniya-konsultant shuni qayd etgan: "Men xavf shaxsiy qurilmalardan foydalanishda to‘planadi deb hisoblayman. Barcha keng ko‘lamdagi funksiyalarni bajaruvchi, simsiz tarmoqlarga ulanuvchi, ishda va shaxsiy hayotda ijtimoiy tarmoqlar va elektron pochta orasida bog‘lanishni hosil qiluvchi vositalarni ish joyiga olib keladi. Shuning uchun, o‘ylashimcha, asosiy xavf muammoni tushunish madaniyatining yo‘qligidadir”.

So‘nggi paytlarda kompaniyalar tomonidan to‘plangan ma’lumotlardan foydalanib hujumlarga javob berish imkoniyatlari ko‘rib chiqilmoqda. Bir qator tashkilotlar korxonalarga huquqbuzarlarning profillarini va ularning hujumlari sabablarini tuzishda yordam beradi. Bu ma’lumotlar, texnik muhofaza qilish va sud jarayonlari sifatini yaxshilash, firibgarlik huquqbuzarni aldash uchun kompaniyalar o‘z tarmoqlarida noto‘g‘ri ma’lumotlarni joylashtirish, hujumni iloji boricha ko‘p resurs talab qiluvchi faoliyatga aylantirish maqsadida qo‘llaniladi. Ba’zi kompaniyalar xakerlarga qarshi qaratilgan "teskari xakerlik hujumi" imkoniyatini ko‘rib chiqmoqdalar, lekin bu qanchalik qonuniy va texnik jihatdan imkoni borligi hali aniq emas.

Umumiy nigohda kiber jinoyatni oldini olish aralash xarakterga ega. Katta kompaniyalar, ayniqsa moliyaviy xizmatlar sohasida, foydalanuvchilarni avtorizatsiya qilish uchun apparat xavfsizligi kalitlari kabi maxsus xavfsizlik texnologiyalaridan foydalangan holda yanada murakkab kiber jinoyatchilikni oldini olish bo‘yicha strategiyalarga rioya qilishadi. Xavfsizlik masalalari bilan shug‘ullanuvchi kompaniyalar faol monitoring olib borshadi va yangi tahdidlar shakllanishi haqida hisobotlarni doimiy e’lon qilib borishadi, bir qator texnologik kompaniyalar esa sudlarga bot-tarmoqlarni yo‘q qilish, spammerlar va firibgarlarni kuzatish to‘g‘risidagi da’volar bilan faol murojaat etishadi. Bundan tashqari, kichik kompaniyalar juda yaxshi himoyalanmagan va ba’zilari xavfsizlik choralari bilan bog‘liq xavflarni aniq tushunchasiga ham ega emas.

Internet xizmatlari va xostingni taqdim etuvchilar tomonidan kiber jinoyatchilikning oldini olish. Internet-insfrastruktaralarida Internet xizmatlarini taqdim etuvchilar alohida o‘ringa ega. Ular yuqori sig‘imli optik tolali kanal va serverlar, kommutatorlar va marshrutizatorlar hamda *radiosotlar* (mobil tarmoq operatorlari holatida) va boshqa asosiy elementlarni sotib oladi yoki ijaraga oladi, bu bilan tarkibni qo‘yish va tarqatish, stol va cho‘ntak uskunalarini Internetga

ulash imkonini beradi. Bir tomondan, xizmat koʻrsatuvchi provayderlar kiber jinoyatlarning oldini olishda rol oʻynashi aniq, ammo boshqa tomondan, xizmat koʻrsatuvchi provayderlarning masʼuliyati va Internet-kontent uchun javobgarlik muammolari ham mavjud. Kiber jinoyatlarning oldini olishda xizmat koʻrsatuvchi provayderlarning imkoniyatlarini koʻrib chiqish uchun birinchi navbatda bir nechta texnik jihatlarni qisqacha tahlil qilish kerak.

Internet-provayderlar foydalanuvchilarni Internetga ulaydi va global tarmoq, elektron pochta va ovozli IP (VoIP) serverlari orqali foydalanuvchilar va qurilmalar oʻrtasida maʼlumotlarni uzatadi. Agar foydalanuvchi virtual xususiy tarmoq, proksi-server yoki maʼlumotlar almashinuvida ishlatiladigan dasturiy taʼminotga biriktirilgan vazifalar yordamida maʼlumotlarni shifrlamasa, Internet xizmati provayderlari baʼzi trafikni tahlil qilishi mumkin. Internet xizmatlarini koʻrsatuvchilar uchun maʼlum boʻlgan foydalanuvchi maʼlumotlariga axborot almashinuvi tarkibi, yaʼni veb-sayt va elektron- pochtadagi shifrlanmagan matnlar va suratlar, kontekstual maʼlumotlar, misol uchun abonent qaysi serverlarga tashrif buyuradi, elektron pochta xabarlarining manbasi va yoʻllanish manzili, turli xizmatlardan foydalanishning vaqti va davomiyligi kiradi. Shu vaqtning oʻzida, bunday maʼlumotlar shifr qoʻllash holatida ham provayder uchun maʼlum boʻladi. Umuman olganda, tarkib faqatgina joʻnatilish vaqtida qoʻllanila oladi, keyinchalik esa faqat foydalanuvchi ulanishlarining aniq monitoring va maxsus qurilmalarni qoʻllagan holda maʼlumotlarni saqlashda amalga oshadi. Istisno sifatida provayder elektron pochta serverini boshqarish holati hisoblandi, negaki bunda xabar uzoqroq muddat saqlanadi.

Bir kishiga koʻpincha bir nechta Internet-provayderlar tomonidan xizmat koʻrsatiladi, chunki kirish turli joylardan amalga oshiriladi. Koʻpincha uy uchun Internet xizmatlarini bitta provayder, mobil qurilmalar uchun esa boshqasi taʼminlaydi. Uchinchi provayder ish joyida Internetga kirish uchun foydalanilishi mumkin va mahalliy kafe ichidagi simsiz tarmoqqa ulanishda boshqa internet-provayder bunday ulanishni taʼminlash uchun ishlatiladi. Shuning uchun, bir shaxsning faoliyati toʻgʻrisida maʼlumot turli xil xizmat koʻrsatuvchi provayderlarga tegishli boʻlishi mumkin.

Yetkazib beruvchi Internet hosting veb-saytlar va boshqa xizmatlarda qoʻllaniluvchi tizimlarni nazorat qiladi. Internet-servis provayderlari va ularning abonentlari oʻrtasidagi munosabatlarda boʻlgani kabi, xizmat koʻrsatuvchi

provayderlar hosting xizmati mijozlarning barcha kiruvchi va chiquvchi trafiklarini kuzatish uchun noyob imkoniyatga ega. Shuning uchun ular bunday xizmatlardan noqonuniy foydalanishni to‘xtatish yoki blokirovka qilish uchun texnik imkoniyatlarga ega. O‘zlarining xizmat shartnomalarida, hosting kompaniyalari, odatda, o‘z serverlarida joylashtiriladigan xizmatlarning tabiatiga, odatda ma’lum miqdordagi spam yoki noqonuniy elektron pochta xabarlarini yuborish, noqonuniy kontentni o‘rnatish yoki mualliflik huquqining buzilishi kabi ma’lum nomaqbul xatti-harakatlarga qo‘yilgan cheklovlarni yoritadi.

Xizmat ko‘rsatuvchi provayderlar ikki asosiy sohada kiber jinoyatlarni oldini olishda muhim rol o‘ynaydilar:

– keyinchalik kiber jinoyat tergovida huquq-tartibot idoralari foydalanishi uchun foydalanuvchi ma’lumotlarini saqlash;

– avvalo kiber jinoyatning oldini olish uchun internetdagi ma’lumotlar almashinuvi yoki ma’lumotlar tarkibini faol «filtrlash».

Ma’lumotlarni saqlab turish. Internet-provayderlar tarmog‘i orqali o‘tadigan trafik miqdori hisobga olinsa, ular barcha trafiklarning to‘liq ro‘yxatini saqlay olmaydilar. Ba’zi mamlakatlar murakkab internet monitoringi tizimlarini joriy qildilar, ammo texnologik cheklovlar tufayli katta hajmdagi ma’lumotlarni to‘plash va tahlil qilish qiyin bo‘lishi mumkin. Unchalik ikir-chikirli ma’lumotni (masalan, ayrim foydalanuvchilarga belgilangan vaqtda berilgan IP-manzillar kabi) ro‘yxatga olish uzoq vaqtni qamrab olishi mumkin. Internet-provayderlar odatda "real vaqtda" ma’lumotlarning manzil monitoringini amalga oshirish imkoniyatiga ega va ho‘pgina mamlakatlardagi "qonuniy ushlab turish" qoidalarini internet-provayderlar odamni yoki xonadagi ulanishlarni real vaqt rejimida to‘liq monitoring qila olishi kerakligini ta’kidlaydi.

Ma’lumotlarni himoyalash. Ko‘p mamlakatlarda Internet xizmatini ko‘rsatuvchi provayderlar tomonidan ma’lumotlarni saqlash va qayta ishlash himoya qilish to‘g‘risidagi qonunchilik tomonidan belgilanadi, u shaxsiy ma’lumotlarni qo‘llash va himoyalashga doir sohada talab qo‘yadi. Xavfsizlik tamoyili shuni belgilaydiki, kartotekalar” noqonuniy kirish, ma’lumotlardan noqonuniy foydalanish va kompyuterlarga virus kiritish kabi inson faoliyati bilan bog‘liq xavflardan holi bo‘lishi kerak”.

Biroq shaxsiy ma’lumotni ma’lumotlarni himoyalash doirasidagi maqsadlar uchun kerak bo‘lmagan shaxsiy ma’lumotlarni o‘chirish majburiyati politsiya organlari tomonidan kiber jinoyatni tergov qilish

jarayoniga ta’sir qilishi mumkin. Masalan, bir qator huquqni muhofaza qilish idoralari internet-provayderlar tomonidan qisqa muddatli ma’lumotlarni saqlab qolish bilan bog‘liq bo‘lgan muammolar haqida xabar berishgan, bu esa ayrim holatlarda ma’lumotlarni himoya qilish to‘g‘risidagi qonun hujjatlari bilan bog‘liq bo‘lishi mumkin. Bundan tashqari, shaxsiy ma’lumotlarni qayta ishlaydigan barcha tashkilotlarga va shaxslarga nisbatan qo‘llaniladigan ma’lumotlarni himoya qilish to‘g‘risidagi qonun hujjatlari Internet-servis provayderlari tomonidan ro‘y beruvchi kiber jinoyatlarning oldini olishda yordam beradi, negaki ular foydalanuvchi ma’lumotlarining xavfsizligi va yaxlitligini ta’minlash uchun ma’lumotlarni qayta ishlash standartlarini belgilab qo‘yadi.

Ma’lumotlarni saqlash. Ma’lumotlarni muhofaza qilish to‘g‘risidagi qonun hujjatlari talablarini katta hajmdagi ma’lumotlarni saqlashning moliyaviy oqibatlari bilan birgalikda hisobga olgan holda, Internet-provayderlar ma’lumotni cheklanmagan vaqt davomida saqlamaydilar. Huquqni muhofaza qilish organlariga tergov o‘tkazishda yordam berish uchun ba’zi mamlakatlarda ma’lumotlar himoyasi to‘g‘risidagi qonun hujjatlariga nisbatan istisnolardan foydalanildi, unga muvofiq Internet-provayderlar Internet-obunachilarning ma’lum turdagi aktivligi to‘g‘risidagi ma’lumotlarini belgilangan vaqt oralig‘ida (masalan, bir yil) saqlaydi, bu vaqt ichida tergov organlari ushbu ma’lumotlardan sud yoki ma’muriy organlarning ruxsati bilan foydalanishlari mumkin.

Ma’lumotlar xavfsizlik tizimlarini zararlanganligi haqida xabar berish. Va nihoyat, "axborot xavfsizligi tizimlariga ziyon yetkazish to‘g‘risida majburiy xabar berish to‘g‘risidagi" talablar Internet-provayderlarning abonent ma’lumotlarini saqlashga ta’sir qilishi mumkin. Ta’sirlangan shaxslarga va tartibga solish organlariga ma’lumotlar xavfsizligi tizimiga yetkazilgan zarar haqida, xususan, shaxsiy ma’lumotlarning oshkor etilganda majburiy bildirishnoma berish bir qator mamlakatlarda keng qo‘llab-quvvatlandi. Bildirishnoma bunday zarar oqibatida zarar ko‘rgan tomonga bunday hodisaning oqibatlarini yumshatish uchun xavfsizlik nuqtai nazaridan maslahatlar berish (masalan, parollarni yoki foydalanuvchining shaxsiy kodini o‘zgartirish yoki to‘lov kartalarini qayta berish uchun murojaat etish), xavfsizlik tizimlarini takomillashtirish uchun kompaniyalarga raqobatbardoshlikni kuchaytirish va ma’lumotlarni muhofaza qilish va hayotiy infrastruktura uchun mas’ul boshqaruvchilarning say-

harakatlarini qo‘llab-quvvatlash chora tadbirlarini ko‘rish imkonini beradi.

Axborot xavfsizligining buzilishi to‘g‘risidagi xabarnomalar axborot xavfsizligi tizimining muhim elementi, shu jumladan Internet-provayderlarga nisbatan, bunday qonunlar «xavfsizlikka ziyon» atamasini belgilashda ehtiyotkor yondashuvni ta’minlab berishi va bir qator boshqa choralar bilan ,jumladan, ma’lumotlarni muhofaza qilishning samarali qonunlari birgalikda ishlatilishi lozim.

Internet-kontentni filtrlash. Internet provayderlari ma’lumotlarni jinoyatchilikning oldini olish uchun yordam berishda saqlash imkoniyatidan tashqari Internetdagi ma’lumot almashinuvi va uzatilayotgan shaxsiy ma’lumotning aktiv tahlilini qo‘llashi mumkin. Bunda asosiy tamoyillardan biri bu internet-provayderlari tomonidan internet-mazmunni “filtrlash” hisoblanadi. Internet-ulanishlarning filtrlanishi har qanday tarmoqda ma’lum darajada o‘rin egallaydi. Faoliyat samaradorligini oshirish va xavfsizlikni ta’minlash uchun qo‘llaniluvchi filtrlashning boshlang‘ich darajasi bu noto‘g‘riyoki boshqa yo‘lda zararlangan ma’lumotni bloklashdir. Internet-provayderlar noqonuniy yoki zararli tarkibni aniqlash maqsadida axborotni filtrash texnik imkoniga ega bo‘lishi mumkin. Masalan, ko‘plab internet-provayderlar o‘zlarining obunachilarining elektron pochta xabarlarini filtrlash va viruslar yoki xakerlar hujumlari bilan bog‘liq ma’lum zararli trafikdan himoya qilish uchun bunday turdagi trafikni tashishdan voz kechib asosiy spam-filtrlardan foydalanishi mumkin.

Spam va bot-tarmoqlar. Spam-filtrlash - kunlik yuborilgan va olingan spam xabarlarning katta hajmini hisobga olgan holda barcha elektron pochta xizmati provayderlari uchun jiddiy muammo bo‘lib kelmoqda. Spam filtrlash vositalari turli va murakkabdir. Bunga ma’lum spam manbalarini aniqlash uchun pochta xabarlarini jo‘natuvchilarni tahlil qilish, shuningdek, standart so‘z birikmalarini va xabarlar tarkibini aniqlash uchun matnlarni tahlil qilish kiradi. Spam sifatida tasniflangan xabarlar ba’zan to‘liq bloklanadi yoki foydalanuvchining "spam-jildiga" yuboriladi.

Internet-provayderlar internet-trafik tuzilishiga yoki xabarnomaga asosan, ularning tarmog‘idagi qurilmaning bot-tarmoqning bir qismi bo‘lib qolgani yoki boshqa xavfli dastur bilan zararlanganligi haqida xabar topganda, mumkin bo‘lgan harakat variantlardan biri ushbu manzildan keluvchi zararli trafik qisman yoki to‘liq blokirovkalash, shu

paytning o‘zida obunachiga zararli dasturni o‘chirish uchun kerakli choralar haqida ma’lumot berishni o‘z ichiga oladi. Bunday xabarnomalar zararli dasturlarni "tuzoq qurilmalari" kabi texnik vositalar yordamida bot-tarmoqlarni aniqlash maqsadia monitoring o‘tkazuvchi xavfsizlik bo‘yicha javobgar kompaniyalardan tomonidan kelishi mumkin. Internet-provayderlar, shuningdek, trafikda taniqli imzolar mavjudligini kuzatish orqali buzilgan qurilmalarni faol aniqlash uchun choralar ko‘rishlari mumkin, ammo bunday harakatlarning samaradorligi uchun ma’lum darajadagi manzillik talab etiladi.

Ma’lumot tarkibini filtrlash. Quyida aytib o‘tilganidek, Internet-provayderlarning majburiyatlari to‘g‘risida gap ketganda, ba’zi davlatlarning qonunlari internet-provayderlar bolalar pornografiyasi kabi noqonuniy kontentdan foydalanishni taqiqlashini talab qiladi. Internet-provayderlar buni amalga oshirishining turli usullari mavjud, turli usullar esa tezlik, harajat, samaradorlik va aniqlik nuqtai nazaridan murosali variantlarni taklif qiladi. *DNS filtrlarini* ishlatish Internet-provayderlarga DNS-serverlarining o‘z abonentlariga yuboradigan javoblarini nazorat qilish va ma’lum bir sahifaga yoki qidiruv natijalari to‘plamiga emas, balki «google.com»kabi domenga kirishni cheklash imkonini beradi. Bunday cheklovlar atrofdagilar tomonidan osonlik bilan chetlab o‘tilishi mumkin, chunki foydalanuvchilar asl natijalarni beradigan boshqa DNS-serverlarini ishlatishlari mumkin.

IP- sarlavhalari bo‘yicha filtrlash alohida kompyuterlarni manzillariga qarab bloklash yoki hatto Internet yoki elektron pochta kabi muayyan xizmatlarni qisman blokirovka qilish uchun ishlatilishi mumkin. Bir internet-serverida bir qator veb-saytlar joylashgan bo‘lishi mumkin, shu sababli bu muammo tegishli bo‘lmagan veb-saytlarga ta’sir qilishi va ba’zan ularning soni juda oshishi mumkin. Internet-trafikning asosiy mazmunini tahlil qilish uchun *chuqurroq ma’lumot paketi tekshiruvidan* foydalanish mumkin. Bu filtrlash uchun juda moslashuvchan yondashuvga imkon beradi, lekin yuqori tezlikdagi ISP-kanallarga o‘rnatilishi kerak bo‘lgan qimmatbaho uskunalarni talab qiladi va bu barcha obunachilar ulanishini sekinlashtiradi. Amaliyotda filtrlashning ko‘plab rejimlari gibrid filtrni hosil qilgan holda ushbu usullarni birgalikda qo‘llashni nazarda tutadi. Masalan, DNS- ga asoslangan oddiy filtrlar odatda murakkab filtrlarni sinab ko‘rish uchun yuborilishi kerak bo‘lgan trafikni aniqlash maqsadida ishlatiladi. Ushbu gibrid yondashuv kerakli resurslarni sezilarli darajada kamaytirish bilan murakkab filtrlashni ta’minlaydi.

Umuman olganda, Internet-provayderlar va hosting provayderlari odamlar va tashkilotlarni Internetga ulagan holda, kiber jinoyatlarning oldini olishda muhim rol o‘ynashi mumkin. Ular jinoiy tekshiruvlarda ishlatilishi mumkin bo‘lgan jurnallarni saqlab turishlari; mijozlarga buzilgan kompyuterlarni aniqlashda yordam berish; spam kabi muayyan noqonuniy kontentlarni bloklash; o‘z mijozlari uchun xavfsiz axborot-kommunikatsiya muhitini yaratishda umumiy yordam berishlari mumkin. Ko‘pgina mamlakatlarda axborotni muhofaza qilish to‘g‘risidagi qonun hujjatlari Internet-provayderlarning mijozlar ma’lumotlarini himoya qilishini talab qiladi va tergov kuchlari politsiyaning bu ma’lumotlardan foydalanishiga mos proporsional belgilanadi. Internetda erkin axborot oqimiga cheklashlarni belgilovchi qonunchilikda so‘z erkinligi prinsipi ham e’tiborga olinishi lozim. Internet-provayderlari va boshqa vositachilar javobgarlikdan himoya qilish onlayn xizmatlarning tez o‘sishida asosiy omil bo‘ldi, lekin Internet-provayderga mualliflik huquqi buzilishi va boshqa qonunbuzarliklardan ogohlantirilgan taqdirda choralar choralar ko‘rish kabi ma’suliyat yuklatildi.

Kiber jinoyatlarning oldini olishda ilmiy jamoatchilik ishtiroki. Ilmiy muassasalari va hukumatlararo tashkilotlar kiber jinoyatning oldini olish va unga qarshi kurashishda muhim rol o‘ynaydi. Bunday muassasalar, xususan, axborot bazasi va bilimlarni almashish, qonunchilik va siyosatni ishlab chiqish, texnologiyalar va texnik standartlarni ishlab chiqish, huquqni muhofaza qilish idoralari bilan texnik yordam ko‘rsatish va hamkorlikni rivojlantirishga yordam berishi mumkin.

Axborot bazasini rivojlantirish va bilimlarni almashish: Davlat muassasalari va xususiy korxonalar tomonidan kiberxavfsizlik sohasida malakali kadrlar va xodimlarni rivojlantirishga bo‘lgan talabga javoban, ilmiy muassasalar bilim va tadqiqot natijalarini mustahkamlash va soha hamda fanlararo birikishning ta’sirini kuchaytirish uchun maxsus o‘quv dasturlari, o‘quv rejalari va kadrlarni tayyorlash markazlari yaratdilar. Kiber xavfsizlik va kiber jinoyatlar sohasida diplomlar, sertifikatlar va o‘quv mashg‘ulotlarini «xavfsiz kompyuter amaliyoti va texnik aspektlari masalalari bo‘yicha yosh mutaxassislar va bo‘lajak ekspertlar uchun ta’lim va professional tayyorlov» maqsadida taklif etadigan universitetlar soni ortib bormoqda. . Seminar va konferensiyalarni tashkil qilish orqali universitetlar shuningdek, kiber jinoyatlarga qarshi kurashish uchun

ijtimoiy tarmoqlarning amaliy ta’limi va rivojlanishini rag‘batlantiradilar. Bunday tadbirlar axborot almashish va jinoyatchilikning oldini olish va javob berish bo‘yicha tavsiyalar beradi, bu esa norasmiy hamkorlikni rivojlantirishga yordam beradi, ba’zida tegishli organlarga ma’lum jinoyatlar haqida axborot berish va texnik yechimlarni ishlab chiqish mexanizmlarini taklif etadi.

Qonunchilik va siyosatni ishlab chiqish: Universitet mutaxassislari loyihalarni ishlab chiqish va qonunchilik, siyosatga o‘zgartirishlar kiritishda katta hissa qo‘shmoqdalar. Milliy, mintaqaviy va xalqaro miqyosda olimlar keng ko‘lamli masalalar, shu jumladan kriminallashtirish, maxfiylik va shaxsiy hayot huquqi, konstitusiyaviy hamda huquqiy himoya qilish masalalari bo‘yicha qonun loyihalarini tayyorlashda maslahat berishadi va ishtirok etishadi. Bunday maslahat turli mexanizmlar orqali, shu jumladan konsultativ va maxsus ishchi guruhlar, institutlar va individual mutaxassislar darajasidagi aloqalarni va texnik yordam dasturlari orqali ta’minlanadi. Ilmiy muassasalardan birining respondentlaridan biri, masalan, maxsus kiber muhit masalalari bilan shug‘ullanuvchi tadqiqot markazlari ko‘pincha " kiber jinoyatlarga oid muammolar (huquqiy, kriminalistik, texnik ekspertiza) bilan bog‘liq bo‘lgan bir qator tor doiralarda tadqiqotchilarning faoliyati" uchun koordinator bo‘lib xizmat qilishi aytgan .

Texnologiyalar va texnik standartlar: Universitetlar kompyuter texnologiyalari sohasida ilmiy ishlarni mahalliy yoki xorijiy homiylarning moliyaviy ko‘magida xususiy sekto va (yoki) davlat tashkilotlari bilan hamkorlikda, yoki universitet xavfsizligini ta’minlash doirasida olib boradilar. Bundan tashqari, universitetlar kompyuter kriminalistikasi, dalillar tahlili va tashkilot ma’lumotlari tahlili kabi yo‘nalishlar bo‘yicha o‘z hissalarini qo‘shishlari mumkin. Universitetlar va alohida mutaxassislar darajasida olib borilgan tadqiqotlar bilan bir qatorda, universitetlar ham standartlar o‘rnatish uchun mas’ul bo‘lgan professional tashkilotlar va tashkilotlarda, hamda texnik ishchi guruhlarda ishtirok etishda hamkorlikning muhim hamkorlar va hamkorlikning tashkilotchilari hisoblanadi.

Huquqni muhofaza qilish idoralari bilan hamkorlik: Huquqni muhofaza qilish organlari rahbarlari universitetlar bilan hamkorlik qilish, universitetlarda kiber jinoyatlarda va kiberxavfsizlik sohasidagi to‘plangan tajribani inobatga olgan holda, hamkorlik qilishdan manfaatdor bo‘lishi mumkin. Oliy o‘quv yurtlari vakillarining respondentlari huquqni muhofaza qilish organlari bilan hamkorlikda

bilimlar bazasini, texnik standartlarni va texnik yordamni ishlab chiqishda hamkorlik qiladilar, biroq ko‘plab ilmiy jamoatchilik vakillari ham huquqni muhofaza qilish idoralari bilan bevosita aloqada bo‘lmaganligini qayd etdilar. Olimlar bunday ta’lim dasturlari va axborot almashinuvini kengaytirish uchun resurslarning mavjudligiga doir muammolar ularni bezovtalikka solishini ta’kidlashadi. Masalan, respondentlardan biri: “Hamkorlik uchun umumiy rasmiy asoslar yo‘q - davlat muassasalari universitetlar bilan hamkorlik qilish uchun standart yoki byudjetga ega emas. Shuning uchun barcha mavjud aloqalar va axborot almashinuvi norasmiydir” deb aytib o‘tgan. Jamoat xavfsizligini ta’minlashda yordam berish uchun “mablag‘ ajratish, xodimlar soni va tor doira mutaxassislarining mavjudligi” ishlashni yaxshilash uchun zarur bo‘lgan omillar sifatida qaraladi, bu ayniqsa "sud ekspertizasi va kriminalistik analiz vositalari, kadrlarni tayyorlash va malakasini oshirish masalalari bo‘yicha moliyalashtirishni oshirish"ga tegishlidir. “Qo‘shimcha resurslar, tartibni saqlash organlari tomonidan hamkorlikka tayyorlikni ko‘rsatish va ilmiy muassasalardagi izlanishlar” ga bo‘lgan talabga qaramay, davlat tashkilotlari va tartibni saqlash organlari bilan hamkorlikni kengaytirishga imkoniyat kattadir.

Kiber jinoyatchilar va kiber-terrorchilar doimiy ravishda yangi amaliyotlarni, dasturiy yechimlarni va texnologik yangiliklarni qabul qilmoqda. Bularning barchasi moliyaviy tizimda yangi shifrlash usullari, transaksiyalar va boshqalar kirib kelishi bilan bog‘liq moliyaviy inqilobning fonida yuzaga keladi. Bunday sharoitda kiberxavfsizlik strategiyasi va ularning tegishli standartlari, protseduralari va dasturiy ta’minoti, shuningdek stressni tahlil qilish va kadrlarni o‘qitish tizimlari davriy tekshirishni va yangilanishni talab qiladi. Kiber xavfsizlik sohasidagi dasturiy ta’minot, apparat, tashkiliy, boshqaruv va kadrlar yechimlari doimiy o‘zgarishi bilan xavflarni ko‘paytirishi, tahdidlarni kuchaytirishi va kiber muhitda tez o‘zgarishga moslashish mumkin. Iqtisodiyotning boshqa moliya sektorlarida, ayniqsa energetika va telekommunikatsiya tarmoqlarida mavjud muammolar, moliyaviy sektorda kiberxavfsizlik holatiga ijobiy yoki salbiy ta’sir ko‘rsatishi mumkin. Shuning uchun moliya institutlarining menejerlari va aksiyadorlari, davlat organlarining yuqori mansabdor shaxslari kiber xavfsizlik masalalarini nafaqat rivojlanish, balki jamiyat, biznes va davlatning omon qolishida muhim masalalar sifatida ko‘rib chiqishlari kerak. Biznes, milliy xavfsizlik, davlat xizmati sohalaridagi har qanday boshqaruv jarayonlarida kiber xavfsizlik masalalari o‘z o‘rnini topishi lozim.

Jinoyatchilikning oldini olish bo‘yicha eng so‘nggi texnologiyalardan foydalanish.

Ayni paytda, Buyuk Britaniyadagi jinoyat bo‘yicha ma’lumot omborlarining kamida 70% ni video va foto-fayllar tashkil etadi. 100 mingdan ziyod aholiga ega Buyuk Britaniya shaharlari va butun mamlakat transport kommunikatsiyalari 100 foizli video kuzatuvga o‘tishi bilan (2018 yildan kechikmay) Buyuk Britaniyada aynan video fayllar jinoyatchilikning oldini olish va tergov qilishda asosiy ma’lumot elementi va materialiga aylanadi. Ayni paytda, Buyuk Britaniyadagi adliya va huquqni muhofaza qilish tizimi oldida nafaqat ushbu chaqiriqqa texnik jihatdan javob berish, balki matn va audio ma’lumot bilan bir qatorda video ma’lumotdan to‘laqonli foydalanishning imkonini beruvchi qurilmalar bilan ta’minlanish vazifasi turmoqda. Britaniya politsiyasi nafaqat dasturiy ta’minotni, balki jismoniy texnologiya kabi katta ma’lumot va texnologiyadan foydalanadi. Ba’zi bir mamlakatlardan farqli o‘laroq, Britaniya jinoyati politsiyadan jihozlanish bo‘yicha quyi turadi. Bu huquqni qo‘llash amaliyotida muayyan afzalliklarni beradi.

Katta ma’lumotlarni tahlil qilish. Elektron qurilmalar yangi ma’lumotlarni aql bovar qilmas tezlikda yaratadilar. Ma’lumotlarning katta qismi jinoyatchilikning oldini olish uchun ishlatilishi mumkin. Agar jamoat avvalo shaxsiy va korporativ ma’lumotlarga kirishga qiziqish ko‘rsatgan bo‘lsa, kelgusi yillarda huquqni muhofaza qilish organlarining video ma’lumotlarini uzatish, to‘lov tizimining protokollari va, albatta, “Internet buyumlar” protokollariga kirishini tartibga solish zarur. Bugungi kunda smartfonlardan olingan geolokatsiya ma’lumotlari bizga juda ko‘p jiddiy jinoyatlarni aniqlash va oldini olish imkonini beradi.

Jinoyatchilikka qarshi kurashda axborot texnologiyasidan foydalanishning keng tarqalganligi va favqulodda vaziyatlar tufayli, quyidagilarni amalga oshirishning imkoni paydo bo‘ldi:

– jinoyatlarning oldini olish uchun videoma’lumotning avtomatik tahlilini amalga oshirish;

– jinoyatlar tergovini 10-30 marotaba jadallashtirish;

– qarorlar qabul qilishni tezlashtirish uchun bashoratni avtomatlashtirish, assotsiativ aloqalari qidiruvi, ma’lumotlarni guruhlash texnologiyasidan foydalanish;

– favqulodda vaziyatlar uchun javob qoidalarini qurish jarayonini avtomatlashtirish;

– voqealar rivojini hamda kuch va vositalarning joylashuvini hozirgi vaqtda namoyon etish.

Sun'iy intellekt. AQShning bir qator shtatlarida politsiya Visual Mining texnologiyasi (vizual tahlil) bilan birgalikda real vaqt rejimida jinoyatchilik bilan bog'liq axborotni belgilash uchun Text Mining texnologiyasining (intellektual matn tahlili) klasterlash va tasniflash usullari va algoritmlarini qo'llaydi , bu avtomatik rejimda jinoyatlarning oldini olish va tekshirish bo'yicha analitik ishlarni sifat jihatdan yangi bosqichda bajarishga imkon beradi. Ushbu imkoniyat real vaqtda jinoiy tahlil qilishning RICAS (Real-time Intelligence Crime Analytics System) aqlli tizimida amalga oshiriladi, u geografik makon, vaqt, yuzlar va hodisalarni bir vizual ekran maydonida bog'lash imkonini beradi.

RICAS - jinoiy ma'lumotlarni tahlil qilishning aqlli tizimi bo'lib, yagona makonda asosiy va eng samarali real vaqtdagi kriminal tahlil va analitik qidiruvning metod va metodiklarini birlashtirgan, bu issiq izlar va avval ochilmagan jinoyatlar bo'yicha jinoyatni fosh qilishning samaradorligi va natijaviyligini oshiradi va kelajakda sodir bo'lishi mumkin bo'lgan jinoyatlarning oldini oladi.

Global navigatsiya tizimi - makon va zamon ma'lumotini belgilashni tartiblash, qonunni muhofa qilish organlari tomonidan olinishini ta'minlovchi metodlar, dasturiy va texnik vositalar majmuidir. Bunady tizimni yaratishdan maqsad tergovni olib boorish va jinoyatning oldini olish jarayonida huquqni muhofaza qiluvchi organlar faoliyatining information-analitik ta'minoti darajasini ko'tarishdir.

Global navigatsiya tizimi - bu makon-zamon ma'lumotni qayta ishlash va uzatish uchun mo'ljallangan daturiy-apparat kompleksi, qabul qilish vositalari to'plami hisoblanadi. Makon-zamon ma'lumotlarni olish uchun vositalar majmuasi quyidagi tizimostilarni o'z ichiga oladi: GLONASS, statsionar aloqa tizimosti vositasi, mobil aloqa tizimosti vositasi, radio chastotani identifikatsiya qilish tizimosti vositasi, videoyozuvlar tizimosti vositasi, murojaat qilish va shaxsiylashtirish tizimosti vositasi.

Neyron tarmoqlari bazasi asosida jinoyatchilarning yuzlarini tanish. 2014 yilda AQSH Federal Tergov Byurosi (FTB) ***tanib olish tizimini yangi avlodi (NGI)*** muvaffaqiyatli ishga tushirilganini e'lon qildi**.** Uning maqsadi fuqarolarning identifikatsiyalash bo'limini

mustahkamlashdir. NGI ning asosiy xususiyati - biometrik ma’lumotlarni avtomatik ravishda qabul qilish va qayta ishlash. Tizim butun mamlakat bo‘ylab CCTV (yopiq elektron televizion tizim) kameralaridan olingan ma’lumot hisobiga ishlaydi. U insonning noyob xususiyatlarini aniqlaydi va ularni ma’lumotlar bazasida saqlaydi. Keyin, jinoyatni tergov qilish paytida, u rasmlarni tez tahlil qilish va buzg‘unchini aniqlashi mumkin bo‘ladi. Biror kishini aniqlash uchun, masalan, yuzidagi xarakterli chandiqni yoki uning tanasidagi tatuirovkani aniqlash kifoya.

Yuzni tanib olishdan tashqari, NGI o‘z shaxsni qo‘z qorachig‘iga qarab aniqlashga qodir. So‘nggi paytlar Amerika qamoqxonalaridagi mahbuslarning ko‘z qorachig‘i suratlari faol ravishda to‘planadi. Nazariy jihatdan, ular jinoyat sodir etgan joyda tajovuzkorlarni aniqlash uchun ishlatilishi mumkin.

Jinoiy xatti-harakatni bashorat qilishning yangi texnologiyalari. Shanxay transport universiteti olimlari jinoyatchilar va qonunga bo‘ysunuvchi fuqarolarning yuzlarini tekshirish uchun turli xil mashina ko‘rish algoritmlarini qo‘lladilar va keyin ular mashina farqni sezish yoki sezmasligini tekshirishdi.

Insondan farqli o‘laroq, tasvirni tasniflash uchun kompyuterlashtirilgan algoritm subyektivlik yuki bilan yuklangan emas, o‘tgan tajriba, irqiy, diniy yoki siyosiy imtiyozlar, jinsi, yoshi va boshqalar bilan bog‘liq his-tuyg‘ular va noaniqliklarga ega emas, u charchamaydi va uyqu yoki oziq-ovqat yetishmovchiligi unga ta’sir etmaydi, deb yozadi Xitoy olimlari. Ular o‘zlarining yuz suratlari asosida jinoiy moyilliklarni bashorat qilishning avtomtlashgan tizimini taklif etmoqda.

Cloud Walk kompaniyasi (XXR), yuzni tanib olish avtomatlashtirilgan, shuningdek potensial jinoyatchilarning xavf darajasini kuzatish uchun katta hajmdagi ma’lumotlarni tahlil qilish va baholashni tizimlarini o‘rgatishni amalga oshiradi. Qurol-yaroq do‘konlariga tashrif buyuruvchilar yoki turli transport markazlariga tez-tez kelib turadiganlar tizim tomonidan belgilanishi ehtimoli yuqoridir. Hatto uy jihozlari do‘koni ham "shubha" ostida qolishi mumkin, chunki bu joylar hukumat tomonidan "yuqori xavfli" zonalar deb hisoblanadi.

"Albatta, agar kimdir oshxona pichog‘i sotib olsa, bu yerda hech qanday jinoyat yo‘q. Lekin agar bu kishi qo‘shimchasiga qop va bolta ham xarid qilsa, keyin u tizim uchun shubhali bo‘ladi" – deydi Cloud Walk kompaniyasi vakili.

Mutaxassislarning fikriga koʻra, bunday tadqiqotlar keyingi oʻrganishlarni talab etadi va agar muvaffaqiyatli boʻlsa, bunday tadqiqot jinoyatni aniqlash va oldini olish uchun yangi vositani taqdim etishi mumkin.

Asosiy xulosalar

Tor maʼnodagi kiber jinoyat (kompyuter jinoyat) – bu kompyuter tizimlari va ular qayta ishlovchi maʼlumotlar xavfsizligiga qarshi qaratilgan elektron operatsiyalar shaklidagi har qanday noqonuniy xatti-harakatlardir.

Keng maʼnodagi kiber jinoyat (kompyuterlarni qoʻllash bilan bogʻliq jinoyat) - bu kompyuter tizimi yoki tarmoq yordamida yoki ular bilan birgalikda amalga oshiriluvchi har qanday noqonuniy harakat, jumladan, kompyuter tizimi yoki tarmoq yordamida maʼlumotning noqonuniy qoʻlga olinishi, taklif qilinishi yoki tarqatilishidir.

Zamonaviy kiber jinoyatchilikning asosi - global axborot-kommunikatsiya texnologiyalarining transmilliy miqyosda yaqinlashuvi jinoyatlarni sodir etish uchun ishlatilishi mumkin degan fikrdir.

Kompyuter maʼlumotlari yoki tizimi maxfiyligi, yaxlitligi, ochiqligiga qarshi qaratilgan, shaxsiy yoki moddiy foyda olish, kompyuter maʼlumotlariga doir shaxsiy yoki moddiy zarar yetkazish maqsadida kompyuterdan foydalanishni nazarda tutuvchi xatti-harakatlar kiber jinoyat hisoblanadi.

Axborot-kommunikatsiya tizimlarini va Internetdan keng foydalanish jinoyatchilar uchun yangi imkoniyatlar yaratdi va jinoyat oʻsishini tezlashtirdi.

Shaxsiy qurilmalardan foydalanishda xavf toʻplanadi. Asosiy xatar bu muammoni tushunish madaniyatining yoʻqligidadir.

Kiber jinoyatlarning oldini olishning eng yaxshi amaliyotlari orasida qonunlarni qabul qilish, samarali rahbarlik, jinoiy adliya va huquqni muhofaza qilish organlari salohiyatini rivojlantirish, xabardorlikni oshirish, hukumatlar, jamoalar, xususiy sektor va xalqaro tashkilotlar darajasida oʻzaro mustahkam bilimlar bazasi va hamkorlikni oʻrnatish kiradi.

Internet va hosting provayderlari kiber jinoyatlarni oldini olishda muhim rol oʻynashi mumkin. Ular jinoiy faoliyatni tekshirishda talab qilinadigan aloqa jurnallarini saqlab turadi; hujum qilingan kompyuterlarni aniqlashda abonentlarga yordam beradi; spam kabi muayyan noqonuniy kontentlarni bloklaydi; va umuman, mijozlari uchun xavfsiz aloqa muhitini taʼminlaydi.

Ilimy tashkilotlar bilim bazasini rivojlantirish va ulashish, adliya bazasi va siyosatni ishlab chiqish, texnologiyalarni yaratish va texnik standartlarni tayyorlash, texnik yordam ko‘rsatish va qonunni muhofaza qiluvchi organlar bilan hamkorlik qilish orqali kiber jinoyatning oldini olishda muhim hamkor hisoblanadi.

Jinoyatning oldini olishda eng so‘nggi texnologiyalar: katta ma’lumotlar tahlili, aqlli tizim, global navigatsiya tizimi, neyron tarmog‘i.

Nazorat uchun savollar

1. *Kiber jinoyatlarning asosini nima tashkil etadi?*
2. *Global tarmoqqa ulanish kiber jinoyatchilikka qanday ta’sir qiladi?*
3. *Kiber jinoyatlarning o‘sishining asosiy sabablari.*
4. *Kompyuter ma’lumotlarining yoki tizimlarining maxfiyligi, yaxlitligi va mavjudligiga qarshi jinoiy harakatlar.*
5. *Kompyuterni shaxsiy yoki moddiy foyda ko‘rish yoki shaxsiy yoki moddiy zarar yetkazish uchun ishlatish bilan bog‘liq voqealarni keltiring.*
6. *Kompyuter ma’lumotlarining mazmuni bilan bog‘liq amallarni bajaring.*
7. *Kiber jinoyatni kriminallashtirish nimani anglatadi?*
8. *"Jinoyatchilikni ogohlantirish" atamasi nimani o‘z ichiga oladi va bu nimaga asoslanadi?*
9. *Internet-provayderlar va xosting tomonidan kiber jinoyatlar bo‘yicha ogohlantirish berish ketma-ketligini tushuntiring.*
10. *Ilmiy jamoatchilikning kiber jinoyatlarning oldini olishda ishtirokini tushuntiring.*

ADABIYOTLAR RO‘YXATI

1. Ўзбекистон Республикаси Президенти 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида» ги Фармони
2. Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе / В. Ю. Агибалов. - М.: Юрлитинформ, 2012.- 152 с.
3. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А., Стеганография, цифровые водяные знаки и стеганоанализ, Монография, 2009 г.
4. Андреев Б.В. Расследование преступлений в сфере компьютерной информации. М.: Юр- литинформ, 2001. 250 с.
5. Бегларян М.Е. Судебная компьютерно-техническая экспертиза: научно-практическое пособие -М.: Юнити-Дана, 2014. 71 с.
6. Белкин А.Р. Криминалистические классификации. -М., 2000.
7. Быстряков Е.Н., Иванов А.Н., Климов В.А. Расследование компьютерных преступлений. Учебное пособие / Саратов: СГАП, 2000. - 112 с.
8. Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. 2002. № 1.С. 4–12.
9. Всестороннее исследование проблемы киберпреступности. Доклад управления организации объединенных наций по наркотикам и преступности. Организация Объединенных Наций, февраль 2013 г.
10. Гаврилов М.В., Иванов А.Н. Осмотр места происшествия при расследовании преступлений в сфере компьютерной информации. – Саратов, СГАП, – 2006, 2008 г. 136 с.
11. Гатин Р.Б. Расследование преступлений связанных с внедрением новейших технологий / Науки и жизнь. 2001 - 45 с.
12. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. - К.: МК-Пресс, 2006. - 288 с.
13. Криминалистика. Учебник / под ред. Ищенко Е.П., Филиппов А.Г. – М.: изд-во «Проспект», 2007.
14. Криминалистическая видеозапись: Учебное пособие (курс лекций) / под ред. Трубицина Р.Ю. – М.: изд-во «Щит и меч», 2004.

15. Криминалистика: учебник для вузов / Т. В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская. - 4-е изд., перераб. и доп. - М.: Норма: Инфра-М, 2014. - 928 с.

16. Криминалистика: информационные технологии доказывания: учебник под ред. В.Я Колдина. М.: Зерцало, 2007. 752 с.

17. Кэрриэ Б. Криминалистический анализ файловых систем. СПб.: Питер, 2006. 480 с.

18. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический аспект. Воронеж: ВГУ, 2001. 255 с.

19. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: ВГУ, 2002. 408 с.

20. Нехорошев А.Б. Компьютерные преступления: квалификация, расследование, экспертиза: в 2 ч. / А.Б. Нехорошев; под ред. В. Н. Черкасова. Саратов: СЮИ МВД России, 2004. Ч. 2. Расследование и экспертиза. 372 с.

21. Нехорошев А.Б., Шухнин М.Н., Яковлев А.Н., Юрин И.Ю. Практические основы компьютерно-технической экспертизы (учебно-методическое пособие). Саратов: Издательство «Научная книга», 2007. – 266 с.

22. Овчинский В.С. Криминология цифрового мира: учебник для магистратуры. - М. : Норма : ИНФРА-М, 2018. - 352 с.

23. Протасевич А.А. Борьба с киберпреступностью как актуальная задача современной науки / А.А.Протасевич, Л.П.Зверянская // Криминологический журнал Байкальского государственного университета экономики и права. 2011. № 3. С. 28–33.

24. Россинская Е. Р. Судебная компьютерно-техническая экспертиза / Е. Р. Россинская, А. И. Усов. -М.: Право и закон, 2001. -416 с.

25. Савельева М.В., Смушкин А.Б. Криминалистика. Учебник. М,: Издательство Издательский дом «Дашков и К». - 2009 г. – 608.

26. Семикаленова А. И. Мобильные телефоны сотовой связи - новые объекты судебной компьютерно-технической экспертизы / А.И. Семикаленова, К.А. Сергеева // Законы России, опыт, анализ, практика. 2011. № 12. С. 89–94.

27. Федотов Н.Н. Форензика. Компьютерная криминалистика. М.: Юридический Мир, 2007. - 432 с.

28. Чернышов В.Н., Сысоев Э.В., Селезнев А.В., Терехов А.В. Технико-криминалистическое обеспечение следствия: Учебное пособие. Тамбов: Изд-во Тамб. гос. техн. ун-та, 2005.

29. Caloyannides M.A. Privacy Protection and Computer Forensics (Second Education). –«Artech House Publishers», 2004.

30. C.Altheide & H. Carvey. Digital Forensics with Open Source Tools, Syngress, 2011. ISBN: 9781597495868. (Required textbook).

31. Carvey H. Windows Forensics and Incident Recovery. O'Reilly, 2004.

32. Computer Forensics: Principles And Practices, 1st Edition By Linda Volonino, Reynaldo Anzaldua, Jana Godwin. 2012.

33. Gottschalk L, Liu J, Dathan B, Fitzgerald S, Stein M. Computer forensics programs in higher education: a preliminary study, SIGCSE Technical Symposium on Computer Science Education, 2005. 203–231.

34. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response – Recommendations of the National Institute of Standards and Technology (NIST), Publ. 800_86. 2006.

35. Keith John Jones, Richard Bejtlich, Curtis W. Rose. Real Digital Forensics. Mit DVD: Computer Security and Incident Response. Addison Wesley Professional, 2006 - Computers - 650 pages.

36. Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis. Digital Crime and Forensic Science in Cyberspace. 2013.

37. Spivey M.D. Practical Hacking Techniques and Countermeasures. – "Auerbach", 2008.

ILOVALAR

Ilova 1. Raqamli kriminalistika apparat vositalarining namunalari

iStorage diskAshur –
Parol bilan himoyalangan qattiq disk

Tugmali PIN-kodga ega himoyalangan flesh xotiralar, bu qurilma ma’lumotlarni ruxsatsiz kirishdan saqlashning eng ishonchli usuli hisoblanadi. Hattoki apparat shifrlovchisi bilan birga diskni o‘girlatilib qo‘yilishi yoki yo‘qotilishi holatlarida ham, agarda disk korpusdan olib tashlangan bo‘lsa ham diskdagi barcha ma’lumotlar begona shaxslar tomonidan o‘qilmasligiga ishonch hosil qilish mumkin.

iStorage diskAshur himoyalangan fleshkasining xususiyatlari:

- PIN kodini kiritish uchun o‘rnatilgan raqamli klaviatura (6-16 belgilar);
- real vaqtda apparat ma’lumotlarini shifrlash;
- keyloggerlar va qo‘pol kuch (*brute force*) hujumlaridan himoya qilish;
- yo‘q qilingach ma’lumotlarni qayta tiklab bo‘lmaydigan;
- suvga va zarbga chidamli alyuminiy sumkasi;
- drayverlarni o‘rnatishni talab qilmaydi;
- barcha turdagi operatsion tizimlar bilan ishlash qobiliyati;
- o‘lchami va og‘irligining kichikligi.

EPOS eFlash –
Flash-xotirasi

Ma’lumotlarning kafolatli yo‘q qilinish xususiyatiga ega EPOS

eFlash barcha flesh xotira yacheykalaridagi, shu jumladan, yashirin va xizmat ko‘rsatish joylaridagi ma’lumotlarni tezda yo‘q qilish imkonini beradi. EPOS eFlash maxsus drayverlar va dasturiy ta’vinotni talab qilmaydi.

Drayver bilan ishlash uchun kompyuterni USB portiga yetkazib berish to‘plamiga kiruvchi kabel yordamida ulash kerak. Ma’lumotni yo‘q qilish uchun faqat flash korpusidagi yashirin tugmani bosish kifoya, bunda qurilma kompyuterga ulangan bo‘lishi kerak.

EPOS eFlash ning asosiy xususiyatlari:

1. Flash faoliyatini qayta tiklash bilan birga ma’lumotlarni kafolatli yo‘q qilish.
2. Maxsus drayverni o‘rnatish talab qilinmaydi.
3. Yuqori tezlikda ma’lumotlarni o‘chirish.
4. Transportirovka jarayonida favqulodda ma’lumotlarni yo‘q qilish uchun avtonom quvvatlanishning mavjudligi.
5. Hajmi va vaznining kichikligi.

LAVINA - Ma’lumotlarni yo‘q qilish qurilmasi

"LAVINA"da xotiraga kuchli elektromagnit zarbaning ta’siriga asoslangan jismoniy ma’lumotlarni yo‘q qilish usulidan foydalanadi. Natijada, tashuvchining barcha domenlari to‘yingan holatga teng ravishda magnitlangan. Bu ma’lumotlar kodlangan magnit o‘tishini yo‘qotilishiga olib keladi. Shunday qilib, tashuvchidagi dastlabki magnit tuzilishining to‘liq qirg‘ini vositaga yozilgan ma’lumotlarning to‘liq yo‘qolishiga olib keladi. “LAVINA”, bundan tashqari, magnit yozuv printsipidan foydalanuvchi boshqa qurilmalarda: ZIP, Jazz-disk, kassetalar va hokazolarda axborotni o‘chirishda qo‘llanilishi mumkin.

Asosiy xususiyatlari:

1. Kuchli elektromagnit impuls bilan tezda (0.1 sek) ma’lumotlar yo‘qolishi.

2. Ma’lumotlarning tiklash imkoniyatisiz ularni yo‘q qilish kafolati.
3. Ma’lumotlarni ham yaroql, ham nosoz tashuvchilarda yo‘q qilish imkoniyati.
4. Ma’lumotlarni ommaviy yo‘q qilish imkoniyati - 100 dona/soatda.
5. Qo‘llashni osonligi.
6. Kichik o‘lcham va kam og‘irligi.

EPOS DiskMaster Portable

EPOS DiskMaster Portable kompyuterlar xizmat ko‘rsatish markazlari, AT xizmatlari va korxonalarning xavfsizlik xizmatlari mutaxassislari uchun qattiq disklarni ishlatish va ularga xizmat ko‘rsatish bo‘yicha kompleks ishlarni amalga oshirishni ta’minlovchi universal vosita sifatida ishlab chiqilgan. Qurilma barcha qattiq disklar, PATA, SATA, eSATA interfeyslari bilan ishlab chiqaruvchi, model va imkoniyatlardan qat'iy nazar ishlash imkonini beradi.

Shu kabi funksionallikka ega dasturlardan farqli o‘laroq, qurilma qattiq disklarining maxfiy maydoni HPA (Host Protected Area) da, shuningdek, sirtdagi nuqsonli qattiq disklarda ma’lumotlarni nusxalash va yo‘q qilishni ta’minlaydi.

EPOS DiskMaster Portable xususiyatlari uni keng ko‘lamdagi ilovalar bilan ishlashini ta’minlaydi:

- xavfsiz saqlash va axborot tarqalishini oldini olishni ta’minlash uchun - qattiq diskdagi ma’lumotni yo‘q qilish uchun;

- AT insidentlarni (computer forensic) tekshirish - qattiq disklardan ma’lumotlar yozishni, shu jumladan HDD ning himoyalangan hududlaridan ma’lumotlarni o‘chirishni muhofaza qilish;
- ma’lumotni tiklash va HDD ni ta’mirlash uchun - zarar yetkazilgan qattiq disklardan ayovchi rejimida ko‘chirib olish, shuningdek nuqsonli tarmoqlarni yashirish uchun.

IM Solo-4 Forensic Super Kit - Ma’lumotlarni ko‘chirib olish laboratoriyasi

IM Solo-4 Forensic, nusxa olishdan avval, o‘rganilayotgan HDD ma’lumotlarini va fayl mazmunini tahlil qilish , shuningdek, telefonlardan, smartfonlardan, kompakt shaxsiy kompyuterlardan va boshqa mobil qurilmalardan ma’lumotlarni to‘plash va tahlil qilishim ikonini beradi .

IM Solo-4 Forensic Super Kit asosiy xususiyatlari:

- *Eng yaxshi tezlik*

IM Solo-4 Forensic ma’lumotlarni nusxa ko‘chirish, ma’lumotni yo‘q qilish, maksimal tezlikda 18 GB/min gacha tezlikda tekshirishni amalga oshirish imkonini beradi.

- *Drayverlarning keng doirasi*

IM Solo-4 Forensic SAS, SATA, e SATA, USB 2.0, SCSI, USB 3.0, FireWire 400/800 qurilmalari bilan ishlashni qo‘llab-quvvatlaydi.

- *Nusxalash usullari*

- Single Copy. Bitta o‘rganilayotgan drayverni bitta qabul qiluvchiga nusxalash va bir vaqtning o‘zida uchta shunday vazifani bajarishi mumkin.
- Multy Copy. Bitta o‘rganilayotgan drayverni ikkita yoki uchta qabul qiluvchiga nusxalash.

- Parallel Copy. Ikkita o‘rganiluvchi drayverni ikki qabul qiluvchiga masalan, RAID katalogidagi ma’lumotlarni olishda nusxalash.
- Drive Spanning. Ko‘p miqdordagi kichikroq qabul qiluvchilarga katta hajmli manbalarni nusxalash.

RoadMASSter-3 X2 - Kriminalistik laboratoriya

ROADMASST-3X2 laboratoriyasi elektromagnit nurlanishdan himoyalanish bilan mustahkamlangan holda maxsus portativ shaxsiy kompyuter, apparat, dasturiy ta’minot asosida ishlaydigan ko‘p funksiyali tizimdir.

RoadMASSter-3 X2 Forensic ning asosiy xususiyatlari va funksiyalari:

- *Ma’lumotlarni nusxalash.* RoadMASSter-3 X2 Forensic deyarli barcha turdagi HDD (SAS, SATA, PATA, SCSI, USB, FireWire), SSD, flesh drayverlar, CD/DVD disklari, RAID massivlari (RAID 0, 1, JBOD), shuningdek, shaxsiy kompyuter va noutbukdan korpusni ochmay ma’lumot olishi mumkin.
- *Ma’lumotlarni tahlil qilish.* Laboratoriya EnCase, FTK, X-Ways Forensics kabi ma’lumotlarni ko‘rish va tahlil qilish uchun maxsus dasturlarni qo‘llab-quvvatlaydi. Bir tashuvchidan ma’lumotni nusxalashda tadqiqotchi bir vaqtning o‘zida boshqa vositalardagi ma’lumotlar va nusxalarni RoadMASSC-3-ga o‘rnatilgan maxsus dasturiy ta’minotdan
foydalangan holda tahlil qilishi mumkin.
- *Ma’lumotlarni yo‘q qilish (o‘chirish).* HDD dan ma’lumotlarni o‘chirish DoD 5220-22M spetsifikatsiyasiga yoki tezkor yagona o‘tkazish rejimiga muvofiq amalga oshirilishi mumkin.

UltraKit III –
Apparat kompleksi

Digital Intelligence kompaniyasi (AQSh) tomonidan ishlab chiqarilgan Digital UltraKit III to‘plami UltraBlock ovoz yozish apparat blokatori to‘liq to‘plami, qo‘shimcha adapter va kirishlardan iborat kriminalistik ahamiyatga ega bo‘lgan axborotlarni tashuvchi - qattiq disklar, turli tashuvchilar, yoki boshqa qurilmalar kabi kompleksni tashkil etadi. Buning uchun to‘plamdan mos kirish interfeysiga ega blokator tanlanadi, so‘ng yozishdan apparat himoya tizimi yordamida siz dastlabki tashuvchining obrazini o‘z kompyuteringizda yaratishingiz mumkin.

Tableau TD3 Forensic Imager -
Yozib olishning blokiratori

TableauTD3 Forensic Imager tarmoqni qo‘llab-quvvatlovchi qurilmadir. Tarmoq orqali ma’lumotlarni yig‘ish, masofadan tartiblash va tarmoqda yozishni bloklash kabi keng tarmoq sozlamalari yordamida xavfsiz veb-interfeysdan foydalanib, qurilmaga masofadan kirishni ta’minlay olish mumkin. Moslashuvchan mahsulot arxitekturasi keng qamrovli foydalanish sharoitlariga ega va qo‘llab-quvvatlovchi sezgir foydalanuvchi interfeysi mavjud, ingliz tili, portugal, ispan, fransuz, nemis va rus tillarini qo‘llab-quvvatlovchi tushunarli foydalanuvchi

interfeysiga ega minimal o‘rganish bilan ishlash imkonini beradi. Rangli sensor ekran ma’lumotlarni kiritishni, jurnallarni ko‘rishni, tarmoqlarga ulanishni soddalashtiradi va sozlash/ishlashni yakunlaydi. Bundan ham osonroq ishlaydigan tashqi USB klaviaturasi mavjud.

Qurilma quyidagi standart operatsiyalarni bajaradi:

- diskdan diskka ma’lumotlarni takrorlash (klonlash);
- DD, .E01, .EX01 yoki .DMG formatlaridan foydalanib disk tasvirini yaratish;
- formatlash;
- ma’lumotlarni o‘chirish;
- dekodlash (bir vaqtning o‘zidagi MD5 va SHA-1);
- HPA / DCO disklarining maxfiy maydonlarini aniqlash va yo‘q qilish;
- disk diagnostikasi.

EPOS BadDrive Adapter - Yozib olishning blokiratori

EPOS BadDrive Adapter - kompyuter va HDD o‘rtasidagi bo‘shliqda joylashgan va interfeys orqali uzatiladigan barcha buyruqlarni qo‘lga oluvchi ixcham asbob. Qattiq diskda xatolik bo‘lmasa, EPOS BadDrive Adapter an’anaviy yozish blokiratori rejimida ishlaydi.

EPOS BadDrive Adapter xususiyatlari uni keng ko‘lamda qo‘llanilishini ta’minlaydi. U quyidagilar uchun ishlatilishi mumkin:

- *AT insidentlarini tekshirishda*. Texnik holati noma’lum bo‘lgan qattiq disklarda xavfsiz (yozishdan himoyalangan) ma’lumotlarni to‘plash va tahlil qilish imkonini beradi.
- *ma’lumotni tiklashda*. Tizimdagi nuqsonlarni yashirish zararlangan HDDlarning oraliq nusxalarini yaratish zaruratini bartaraf etadi.
- *kompyuter texnikasiga xizmat ko‘rsatganda* . Qurilma ma’lumotlarni "bo‘lingan" qattiq diskga tezda kirish va nusxalash imkonini beradi.

XRY Tablet - Kriminalist-ekspertlar uchun planshet

XRY Tablet - yuqori tezlikda ma’lumotlarni qo‘lga kiritish va soddalashtirilgan foydalanuvchi interfeysiga ega ko‘chma va qulay mobil terminal. U tezkor xizmat vakillariga real vaqtda ma’lumot va analitik axborotni tahlil qilish imkonini beradi, dastlabki baholash jarayonini jadallashtirishga, tergovchilarga va operativ xizmat xodimlariga ma’lumotlarga tezkorlik bilan kirishga imkon beradi, ammo murakkab uskunalar faqat yuqori malakali kadrlar tomonidan ishlatilishi mumkin.

Planshet mobil qurilmalardan kabel va Bluetooth orqali mantiqiy va ma’lumotlarni olishni qo‘llab-quvvatlaydi. Qo‘lga olingan va tahlil qilingan ma’lumotlarni XRY Viewer maxsus namoyish etish vositasi orqali ko‘rish va o‘rganish mumkin. Samarali qidirish funksiyasi va ishlatish uchun qulay grafikalar chiqarilgan ma’lumotlarning ma’lum tanlangan qiymatlarini aks ettirish imkonini beradi. Qo‘lga kiritish jarayonida har doim qurilmadan olingan barcha ma’lumotlarni o‘z ichiga olgan kriminalistik jihatdan xavfsiz XRY fayl yaratiladi.

Cellebrite UFED TK Kompleksi

Cellebrite kompaniyasi taqdim etgan ushbu kompleks yechim yuqori chidamli kompyuterlarning turli modellariga oldindan

o‘rnatilgan, kriminalistik tahlillarga mo‘ljallangan mobil ilova. UFED TK - kerakli tashqi qurilmalar va aksessuarlar komplekti bilan jihozlangan maxsus ko‘rpusda joylashgan portativ kompleks hisoblanadi.

CellebriteUFED TK ning xususiyatlari:

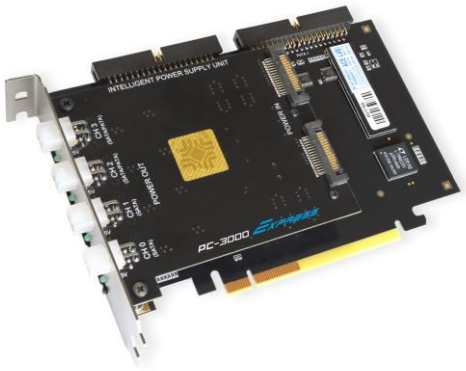
- Android qurilmalaridan, shu jumladan, Samsung Galaxy S, LG, HTC, Motorola va boshqalar oilasidan grafik kalitni/parolni/PIN kodni kiritish orqali blokirobkani chetlab o‘tgan holda ma’lumotlarni olish va dekodlash.
- Android bazasidagi qurilmalardan fizik va fayl tizimi darjasida ma’lumotni qo‘lga kiritish va dekodlash.
- Blokirovka qilingan Nokia BB5 qurilmalaridan fizik ekstraksiya qilish va dekodlash - tanlangan qurilmalardan parolni chiqarish.
- Bloklangan Nokia BB5 vositalaridan fizik darajada qo‘lga kiritish va dekodlash- tanlangan qurilmalardan parolni chiqarish.
- Foydalanuvchi bloklash kodini chetlab o‘tish, ochish yoki o‘chirish orqali bloklangan qurilmalarga oson ulanish.
- Windows Phone, HTC, Samsung, Huawei va ZTE tizimidagi fayl tizimi darajasida chiqarib olish.
- Dekodlash variantlarining boy tanlovi: dastur ma’lumotlari, parollar, elektron pochta, qo‘ng‘iroqlar jurnali, SMS, kontaktlar, taqvim, multimedia fayllari, manzil ma’lumotlari va boshqalar.
- UFED Physical Analyzer orqali murakkab tahlil qobiliyati, jumladan, xronologiya, loyiha analitikasi, zararli dasturlarni aniqlash va nazorat ro‘yxatlari.
- UFED Physical Analyzer yordamida turli formatlarda qulay hisobot yaratuvchisi generator.

XRY Physical mahsuloti

XRY physical kriminalistik ekspertiza mutaxassislariga ma’lumotlarni jismoniy olish yo‘li bilan tergov chegarasini

kengaytirishga imkon beradi, bu esa odatda telefon xotirasida xash damplarni qurilma operatsion tizimidan aylanib o‘tib amalga oshiriladi. Ko‘pincha bu o‘chirilgan ma’lumotni saqlab qolish imkonini beradi.

XRY Physical ichki xotira va tashqi tashuvchidan ma’lumotlarni olish imkonini beradi. Bundan tashqari, XRY Physics xotira tarkibining nusxasini, shuningdek alohida-alohida parollangan fayllarni xash qiymatlarini yaratishni qo‘llab-quvvatlaydi. Ishlab chiqaruvchilar guruhining keng bilimlari tufayli MSAB har bir telefonning noyob xotira tizimini to‘liq tushunadi.



PC-3000 Express - Dasturiy-apparat kompleksi

PC-3000 Express dasturiy-apparat kompleks SATA (Serial ATA) va PATA (IDE) interfeyslari bilan diagnostika va ta’mirlash (faoliyatni qayta tiklash) uchun mo‘ljallangan.

PC-3000 paketiga kiritilgan barcha ixtisoslashtirilgan vositalar quyidagilarni bajarishga imkon beradi:

- texnologik rejimda HDD diagnostikasi;
- HDD xizmat ma’lumotlarini tekshirish va tiklash;
- Flash ROM HDD tarkibini o‘qish va yozish ;
- xizmatga kirish dasturini yuklab olish - LRD;
- P-varaq, G-varaq, T-varaq va hokazo yashirin xatolar jadvalini ko‘rish;
- magnit disklar yuzasida nuqsonlarni yashirish;
- konfiguratsiya va identifikatsiya parametrlarini o‘zgartirish;
- loglarni va S.M.A.R.T. parametrlarini tiklash;
- qattiq diskda o‘rnatilgan parolni ko‘rish va o‘chirish;
- Data Extractor bilan birga ishlash.

Ilova 2. Raqamli kriminalistika dasturiy vositalarining namunalari

X-Ways Forensics

X-Ways Forensics - ma’lumotlar yig‘ishdan tortib to generatsiyaga qadar kompyuter ekspertizasi va AT insidentlar bo‘yicha tergov topshiriqlarining deyarli barcha turlarini tezda hal qilishga imkon beruvchi integrallashgan kompleks hisoblanadi. Bu mutaxassislarning ish samaradorligini oshiradi, tadqiqot vaqtini sezilarli darajada pasaytiradi.

X-Ways Forensic ning asosiy xususiyatlari va imkoniyatlari:

1. Ma’lumotlarni to‘plash va qayta tiklash

- o‘rganilayotgan tashuvchini himoya qilish;
- tashuvchi tasvirlarini yaratish va tiklash;
- JBOD, RAID 0, RAID 5, RAID 6 va boshqa modifikatsiyalari darajasida apparat va dasturiy RAID massivlarida ma’lumotni qayta tiklash;
- tasvir fayllarini ochish va ichki fayl tizimining darajasida ularning tarkibini o‘zgartirish qobiliyati;
- RAM (RAM) operativ tizim va ishlaydigan jarayonlarning virtual xotiralarini ko‘rish va yaratish;
- o‘zlarining ichki tuzilmalari orqali fayllarni qayta tiklash uchun doimiy ravishda yangilangan imzolar bazasi;
- turli xil tashuvchilarda ma’lumotlarni yo‘q qilish.

2. Ma’lumotlarni ko‘rish va tahlil qilish

1. Ichki shablonlarga asoslangan mantiqiy ma’lumot strukturalarini tahlil qilish va tahrirlash.

2. Arxivlarning mazmunini (ZIP, RAR, ARJ, GZ, TAR, 7Zip, BZIP) to‘g‘ridan-to‘g‘ri oldindan ko‘rish oynasida namoyish etish.

3. Belgilangan vaqt oralig‘ida video-yozuvdan statik kadrlarni yaratish imkoniyati.

4. Boshqa hujjatlardagi rasmlarni avtomatik ravishda qidirish va chiqarish (masalan, MS Office hujjatlari, PDF, jpeg rasmlar va hokazo).

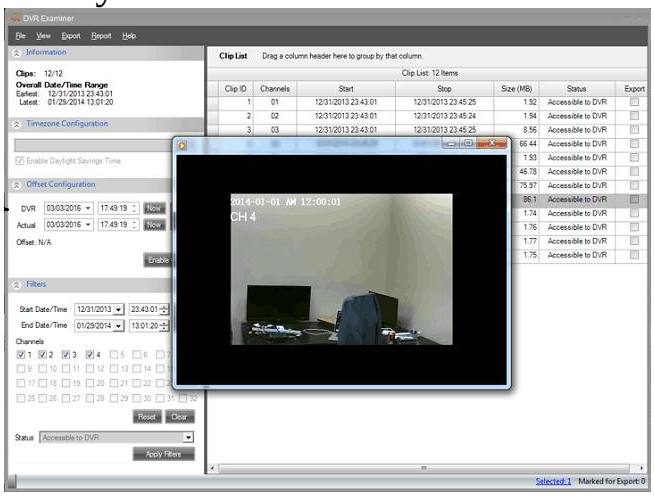
5. Siqilgan va shifrlangan fayllarni avtomat tarzda identifikatsiya qilish

(arxivlar, MS Office hujjatlari, PDF).

6. Shifrlangan va parol bilan qulflangan fayllar uchun parollarni tanlash uchun lug‘at yaratish imkoniyati.

3. Interfeys va moslik

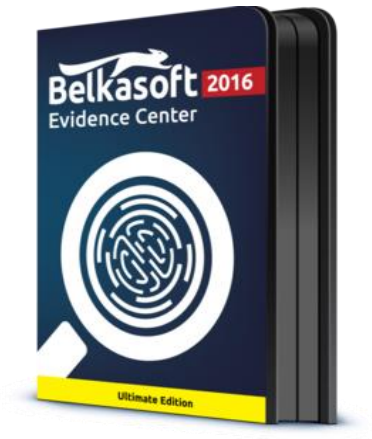
- Qulay vazifa va tergovni boshqarish tizimi.
- Boshqa tergovchilarning barcha metadatalarini tahlil qilish uchun tegishli fayllarni saqlash va uzatish uchun maxsus konteyner fayllarini qo‘llab-quvvatlash.
- Tasvirlarni galereya sifatida ko‘rish.
- Fayllarni yaratish, o‘zgartirish, so‘nggi foydalanish tarixi bilan taqvim sifatida ko‘rish.
- HTML shaklida hisobot yaratish qobiliyati bilan barcha tranzaktsiyalarni avtomatik ro‘yxatga olish.
- Qattiq diskdagi yashirin joylarni aniqlash (HPA).
- WinFE asosida yuklash diski yoki flashdan ishga tushirish imkoniyati.



DVR Examiner – videoregistratorlardan ma’lumotlarni kriminalistik olish va qayta tiklash

DVR Examiner (DME Forensics) video va boshqa metama’lumotlarni videoregistratorlardan, kriminalistik aniqlikka ega video kuzatuv tizimlaridan ma’lumotni olish yechimidir. DVR Examiner

dasturi ekspertlarga videoregistratorga o‘rnatilgan parolni chetlab o‘tib, DVR vositasi qattiq diskidan ma’lumotni bevosita qo‘lga kiritish imkonini beradi. Mahsulot CCTV DVR qurilmalari bilan ish olib boradi va kriminalist mutaxassislar uchun foydali hisoblanadi.



Belkasoft Evidence Center

Belkasoft Evidence Center kriminalist-ekspertlarga bir necha daqiqada yashirin va yo‘q qilingan dalillarni topishda yordam beradi.Yuzlab turli xil artefaktlarni qo‘llab-quvvatlash vositasi ofis formatlari, onlayn suhbatlar, ijtimoiy tarmoqlardagi hujjatlarni, veb-pochta , ko‘plab onlayn-o‘yinlar orqali suhbat , brauzer tarixi va piring jamiyatida almashilgan fayllari aniqlash va qo‘lga kiritish, kriminalistik muhim ma’lumotni izlash va belgilash bo‘yicha keng imkoniyatlarni beradi: mavjud fayllarni o‘rgatish, ularni ichki tuzilishi bo‘yicha tiklash, xotira damplari, gibernatsiya va tortish fayllarning operativ tahlil, PCAP-fayllar ko‘rinishidagi qo‘lga kiritilgan trafikni o‘rganish va hokazo.

Belkasoft Evidence Center dasturi elektron pochta, ijtimoiy tarmoqlardagi faoliyat yoki onlayn o‘yinlardagi xatoliklar - har xil fayllarni tekshirish uchun vaqt sarflaydigan harakatlarni avtomatlashtirish orqali kompyuter jinoyatlarini tekshirish jarayonini sezilarli darajada tezlashtiradi.

Belkasoft evidence Center xususiyatlari:

- O‘rganilayotgan axborot vositasini yozib olinishdan himoyalash.
- Barcha asosiy brauzerlar, elektron pochta mijozlari, ijtimoiy tarmoqlar va fayl uzatish tizimlarini o‘z ichiga olgan 230 dan ortiq artefaktlarni qo‘llab-quvvatlaydi.
- Pornografiya, yuz va matn mavjudligiga video va rasm fayllarini tahlil qiladi.
- Yashirin ma’lumotlar va keng tarqalmagan formatdagi fayllarni qidirish va tahlil qilish.

- O‘chirilgan fayllarni qayta tiklash.
- Bir vaqtning o‘zida bir nechta foydalanuvchilarning ishlashi.
- Sudga dalil sifatida taqdim etilishi mumkin bo‘lgan hisobotlarni tuzish.

Paraben Phone Recovery Stick

Paraben Phone Recovery Stick matnli xabarlar (SMS), IM xabarlari, kontaktlar, qo‘ng‘iroqlar tarixi, internet tarixi va taqvim yozuvlari kabi o‘chirilgan ma’lumotlarni saqlaydi. Telefonni tiklash uchun tayoqni ishlatish oson, oddiy ko‘rsatmalarga rioya qilish kifoya. Qurilmadan iloji boricha tezroq (xotira miqdori, mavjud ma’lumotlar va kompyuterning tezligiga qarab10 daqiqadan 2 soatgacha) ma’lumotlar chiqariladi.

Xususiyatlari:

1. O‘chirilgan ma’lumotlarni qayta tiklash - telefon va SD-kartadan to‘g‘ridan-to‘g‘ri o‘chirilgan ma’lumotlarni saqlaydi. U faqat matnli xabarlarni, Facebook, Chrome, TextFree va boshqalar kabi ilovalardan o‘chirilgan axborotni saqlab qololmaydi.

2. Barcha foydalanuvchi ma’lumotlarini olish - foydalanuvchi ma’lumotlarini yuklaydi va ularni oson o‘qiladigan formatda ko‘rsatadi, hamma narsalarni, onlayn tarixdan Facebookdagi do‘stlariga, Skype-yozishmalarga, qo‘shilmalarini tekshiradi.

3. Xavfsizlik manbasi. Sud ekspertizasining birinchi qoidasi asl ma’lumotlarning saqlanishi hisoblanadi. Phone Recovery Stick mobil kriminalistika qurilmasiga qurilganligi sababli, foydalanuvchi o‘rganilayotgan telefon ma’lumotlari xavfsiz ekanligiga ishonch hosil qilishi mumkin. Telefonda ROOT huquqlarini olishning hojati yo‘q.

Ilova 3. Raqamli kriminalistika dasturiy va apparat vositalarini ishlab chiqaruvchilari to‘g‘risida ma’lumot

	ACE Laboratory (OOO NPP ASE, Rossiya) - HDDni ta’mirlash, shikastlangan HDD dan ma’lumotlarni uzatish, ma’lumotlarni HDD ga ko‘chirish uchun maxsus uskunalar va dasturiy ta’minot.
	Intelligent Computer Solutions, Inc. (AQSh) - qattiq disklardan yuqori tezlikda kriminalistik ma’lumotlarini yig‘ish uchun uskunalar. Kompaniya mahsulotlari AQSh va boshqa mamlakatlardagi huquqni muhofaza qilish idoralari bilan hamkorlikda ishlab chiqilgan.
	Decision Group (Tayvan) - Internet-resurslardan foydalanishni nazorat qilish, axborot tarqalishining oldini olish, yo‘qolgan ma’lumotlarni tahlil qilish va tiklash, kompyuter jinoyatlarini va voqealarni tergov qilish uchun keng qamrovli dasturiy ta’minot va apparat.
	Guidance Software Inc. (AQSh) -" EnCase" kompyuter insidentlarini o‘rganish bo‘yicha jahonga mashhur dasturiy ta’minotni ishlab chiqaruvchi - korxonalar, hukumat va huquqni muhofaza qilish tashkilotlari uchun dasturiy vositalar turkumi.
	Cellebrite Mobile Synchronization Ltd. (Isroil) – telefonlar, smartfonlar, planshetlar va boshqa ko‘chma qurilmalardan ma’lumotlarni chiqarish, ularni dekodlash va tahlil qilish uchun kriminalistika uskunalari sohasida yuqori samarali yechimlar.
	Tableau (AQSh) - kompyuterda insidentlarini tekshirish vositalari: nusxa ko‘chirish qurilmalari, apparat blokerlari, apparat tezlatgichlari va dasturiy ta’minot.
	eDEC Digital Forensics - (AQSh) - sohadagi so‘nggi ishlanmalardan so‘ng kompyuterlar uchun kriminalistika qurilmalari va dasturiy ta’minoti. Kompaniya Xitoyda ishlab chiqarilgan smartfonlardan ma’lumotlarni olib tashlash vositasi bilan mashhur.
	iStorage Limited (Buyuk Britaniya) - bevosita parol kiritish va saqlanadigan ma’lumotni shifrlash xotira vositalari.

	Barracuda Networks, Inc. (AQSh) - barcha o‘lchamdagi tashkilotlar uchun elektron pochta va boshqa tarmoq ilovalari xavfsizligini ta’minlash uchun keng tarmoqli qurilmalar va bulutli xizmatlar.
	**X-Ways Software Technology AG (Germaniya)** – Kriminalistik dasturiy ta’minot. Kompaniyaning mahsulotlari kompyuter insidentlarini tekshirish, ma’lumotlarni qayta tiklash va chuqur tahlil qilish, axborotni kafolatli olib tashlash uchun mo‘ljallangan.
	NRTeam (NAND Recovery Team, Rossiya) - Flash xotiralardan dasturiy va apparat ma’lumotlarini tiklash vositalari. Eng mashhur laboratoriya loyihasi Flash xotiralardan mantiqiy ma’lumotni tiklash uchun Dumppicker dasturi.
	Rapid7 (AQSh) - axborot xavfsizligi xatarlarini tahlil qilish, aniqlash va kamaytirish uchun turli funksiyalarga ega mahsulotlarni qayta ishlash hamda turli axborot xavfsizligi standartlariga muvofiqligini tekshirish.
	Secusmart GmbH (Germaniya) - mobil aloqaning apparat va dasturiy shifrlashi: qo‘ng‘iroqlar, SMS va elektron pochta. birga Germaniya xavfsizlik Federal idorasi (BSI) va mobil telefon ishlab chiqaruvchilari bilan birga mahsulotlarini ishlab chiqaradi.
	BelkaSoft (Rossiya)–tezkor xabarlarning tarixlari, Internet-brauzerlar, mijozlarning pochta qutilari, ijtimoiy tarmoqlarga tashrif izlari, video va tasviriy fayllardagi raqamli dalillarni izlash va tahlil qilishni ta’minlovchi kompyuter ekspertizasi uchun mo‘ljallangan dastur.
	Addonics (AQSh) - xavfsiz modulli ma’lumotlarni saqlash tizimlari, saqlash qurilmalari, duplikatorlar va interfeyslarni o‘zgartiruvchilarga ma’lumotni shifrlash vositalari. Kompaniya tomonidan ishlab chiqilgan texnologiyalar barcha turdagi apparat va operatsion tizimlar bilan maksimal muvofiqlikni ta’minlashga mo‘ljallangan.
	Amped Software (Italiya) - raqamli fotosuratlar va videolarni kriminalistik o‘rganish uchun dasturiy ta’minot. Kompaniyaning mahsulotlari dunyodagi davlat va xususiy tashkilotlarning kriminalist - ekspertlari tomonidan qo‘llaniladi.

Ilova 4. Noqonuniy xatti-harakatlar turlari

Kompyuter ma’lumotlari va tizimlari maxfiyligi, butunliligi, ochiqligiga qarshi qaratilgan xatti-harakatlar	
Kompyuter tizimiga noqonuniy kirish	Kompyuter tizimiga to‘liq yoki qisman noqonuniy yoki asossiz kirish bilan bog‘liq xatti-harakatlarni ifodalaydi. Huquqbuzar xavfsizlik devorini chetlab va bankning kompyuter tizimiga kiradigan holatlar shunga misol bo‘ladi. Bu shuningdek, foydalanuvchining belgilangan vaqtdan tashqari kompyuter tizimiga ulangan holatlariga, masalan, agar huquqbuzar serverning ma’lum bir vaqt uchun faoliyatini saqlab qolsa, bu muddat tugagandan so‘ng ularni ishlatishda davom etadigan holatlar ham bo‘lishi mumkin. Ba’zi mamlakatlarning qonunchiligi jinoyatchining himoya choralarini chetga surishi yoki qasddan harakat qilishi kerakligi ko‘zda tutilgan.
Kompyuter ma’lumotlariga noqonuniy kirish, ushlab qolish yoki sotib olish	Kompyuter ma’lumotlaridan noto‘g‘ri yoki asossiz foydalanish, shu jumladan uzatish jarayonida keng jamoatchilik uchun mo‘ljallanmagan ma’lumotlarni olish, shuningdek, kompyuter ma’lumotlarini ruxsatsiz qabul qilish bilan bog‘liq harakatlar hisoblanadi. Masalan, bu jinoyatchi kompyuterning ma’lumotlar bazasiga noqonuniy kirib kelganligi, uzatilgan ma’lumotni simsiz tarmoqda noto‘g‘ri yozib turishi yoki ma’lum bir firma uchun olib ketish maqsadida fayllardan ruxsatsiz nusxa ko‘chirish hollarni o‘z ichiga oladi.
Noqonuniy ma’lumotlar aralashuvi yoki tizim aralashuvi	Bular kompyuter tizimining ishlashiga to‘sqinlik qiladigan harakatlar, shuningdek, kompyuter ma’lumotlarini noqonuniy yoki asossiz ravishda yo‘qotish, olib tashlash, buzish, o‘zgartirish yoki bloklash bilan bog‘liq harakatlardir. Masalan, huquqbuzar kompyuter tizimiga juda ko‘p so‘rovlar yuboradigan holatlar mavjud ("xizmat ko‘rsatishni rad etish" deb ataladigan hujum), Internet-serverning ishlashi uchun zarur bo‘lgan kompyuter dasturlarini o‘chiradi yoki kompyuter ma’lumotlar bazasidagi

	yozuvlarga o‘zgarishlar kiritadi. Ayrim mamlakatlar qonunlarida ma’lumotlar bilan bog‘liq bo‘lgan amallarni bajarish normalari mavjud, boshqa mamlakatlarda qo‘shimcha qurilmalarga tegishli harakatlarga nisbatan normalar belgilanadi. Kompyuter tizimlariga noqonuniy aralashish muhim infrastruktura (masalan suv yoki elektr ta’minoti) ma’lumotlarga yoki tizimlarga zarar etkazilishiga noqonuniy aralashuvga olib kelishi mumkin.
Kompyuterlardan noqonuniy foydalanish vositalarini ishlab chiqarish, tarqatish yoki saqlash	Kompyuter jinoyatlarini yoki Internetga aloqador jinoyatlar uchun ishlatilishi mumkin bo‘lgan apparat yoki dasturiy ta’minotni ishlab chiqish yoki tarqatish bilan bog‘liq bo‘lgan harakatlar. Masalan, jinoyatchiga xizmat ko‘rsatishni inkor etishni avtomatlashtirish dasturini ishlab chiqadigan hollarni o‘z ichiga oladi. Bunday vositalardan qonuniy foydalanishga aralashishga yo‘l qo‘ymaslik maqsadida (masalan, xavfsizlik bo‘yicha mutaxassislar tomonidan) ba’zi mamlakatlar qonunlari bunday vositalar faqat noqonuniy maqsadlar uchun mo‘ljallangan bo‘lishi yoki jinoyatchini jinoyatlar uchun ushbu vositalardan foydalanish niyati bilan harakat qilishi kerakligi nazarda tutilgan.
Maxfiylikni buzish va ma’lumotlarni himoya qilish choralari	Ma’lumotlarni muhofaza qilish qoidalarini buzgan holda shaxsiy ma’lumotlarni yig‘ish, tarqatish, olish yoki ulardan foydalanish uchun kompyuter tizimidan foydalanish bilan bog‘liq xatti-harakatlarni ifodalaydi. Misol uchun, bu jinoyatchning onlayn-savdoda ishtirok etgan va o‘z ma’lumotlarini oshkor qilmaslik kerak bo‘lgan mijozlar ma’lumotlar bazasidan oshkor qilgan holatlarini o‘z ichiga oladi.
Kompyuterli firibgarlik yoki soxtalashtirish	Kompyuter tizimiga yoki ma’lumotni noto‘g‘ri yoki adolatsiz ravishda olish, boshqa iqtisodiy manfaatlar yoki majburiyatlardan qochish, shuningdek, kompyuter tizimiga aralashish bilan bog‘liq xatti-harakatlar yoki ishonchsiz axborotni yaratishga olib keladigan ma’lumotlar uchun, kompyuter ma’lu-

	motlari. Masalan, jinoyatchining bank tomonidan pul o‘tkazmalarini o‘z hisobiga yo‘naltirishga qaratilgan dasturda o‘zgartirishlar kiritilgan holatlar mavjud yoki jinoyatchining mol-mulkni noto‘g‘ri ishlatish uchun moliyaviy muassasadan dastlabki elektron pochta manziliga o‘zgartirishi mumkin bo‘lgan holatlar mavjud. Shaxsiy ma’lumotni olish yoki mablag‘larni haqorat qilish maqsadida ko‘plab bunday xabarlarni taqsimlash fishing deb ataladi. Kompyuterni firibgarligiga kelsak, ayrim mamlakatlar qonunchiligida dastlabki kompyuter ma’lumotlari qonuniy majburiyatlarni shakllantirishga qaratilgan hujjatlarga tegishli bo‘lishi kerak. Boshqa mamlakatlarda huquqbuzar harakatlar qonuniy majburiyatlarga bog‘liq ravishda ko‘rib chiqilgan yoki qo‘llanilgan o‘zgartirilgan nusxasini olish maqsadida harakat qilishlari kerak.
Shaxsiy ma’lumotlarni ishlatish bilan bog‘liq kompyuter jinoyatchiligi	Bu noqonuniy xatti-harakatni sodir etish, amalga oshirishda qatnashish yoki osonlashtirish maqsadida kompyuter ma’lumotlarida saqlanayotgan boshqa shaxsni identifikatsiya qilish vositalarini noqonuniy o‘tkazish, saqlash yoki ishlatish bilan bog‘liq bo‘lgan harakatlardir. Masalan, bunga jinoyatchining noqonuniy ravishda haydovchilik guvohnomasini kompyuter tizimidan olganligi yoki jinoyatlarda uning haqiqiy identifikatsiyasini yashirish uchun foydalanishi yoki bu ma’lumotni sotayotgani ham kiradi. Ba’zi mamlakatlar qonunlarida ushbu qoidalardan foydalanish shaxsiyligini tasdiqlovchi hujjatlar bilan chegaralanadi.
Mualliflik huquqi yoki tovar belgilari bilan bog‘liq jinoyatlar	Bu kompyuterda saqlanadigan materiallarni nusxalash yoki mualliflik huquqi va tovar belgilarini buzgan holda kompyuter ma’lumotlarini ishlab chiqarish bilan bog‘liq amallar hisoblanadi. Masalan, bu huquqbuzar muallifning mualliflik huquqi egasi tomonidan beriladigan litsenziya bo‘lmasa, faylni taqsimlash tizimida mualliflik huquqi bilan himoyalangan qo‘shiqni tarqatadigan hollarni o‘z ichiga olishi mumkin.

Spam tarqatish yoki boshqarish	Bular kompyuter tizimidan ruxsatsiz yoki nomaqbul xabarlarni juda ko‘p miqdordagi qabul qiluvchilarga yuborish uchun ishlatiladigan harakatlardir. Xo‘jalik yurituvchi subyektlarning mijozlari bilan an’anaviy muloqot qilish jarayoniga aralashmaslik uchun ba’zi mamlakatlar qonunlarida spam sifatida xabarni tasniflash uchun jinoyatchi sarlavhada noto‘g‘ri ma’lumotlar ko‘rsatishi kerak.
Shaxsiy zarar yetkazish uchun kompyuterdan foydalanish bilan bog‘liq xatti-harakatlar	Bu shaxslar uchun ta’qib, ta’qib qilish, qo‘rqitish yoki tahdid qilish maqsadida kompyuter tizimidan foydalanish bilan bog‘liq harakatlardir. Masalan, bu jinoyatchining zararli, tahdid qiluvchi, tajovuzkor yoki tajovuzkor xabarlar yoki tasvirlar (shuningdek, " trolling " deb nomlangan) yoki kuzatuv, bezovta qilish yoki boshqa tekshiruvlar o‘tkazish yoki insonning hissiy va jismoniy holatiga aralashish uchun kompyuter tizimidan foydalanadigan holatlar ham kiradi. Faqat buzilish holatlarida ushbu toifaga kiritilmaydi.
Irqchilik yoki ksenofobiya (chet elliklarga dushmanlik munosabati) bilan bog‘liq kompyuter jinoyatlari	Bu irqchi yoki ksenofobik tarkib yoki tahdidlar yoki irqchilik yoki ksenofobik sabablarga ko‘ra kishilarga nisbatan tahqirlash yoki tarqatish uchun kompyuter tizimidan foydalanishga qaratilgan harakatlardir. Irqiy yoki ksenofobiy materiallar irqi, rangi, kelib chiqishiga shuningdek, diniga, agar ular ushbu omillardan birortasi uchun bahona sifatida ishlatilsa asoslangan har qanday shaxs yoki guruhga nisbatan nafrat, kamsitish yoki zo‘ravonlikni qo‘llab-quvvatlovchi, targ‘ib qiluvchi yoki qo‘zg‘atadigan har qanday yozma materiallar, tasvirlar yoki g‘oyalar yoki nazariyalarni nazarda tutadi.
Bolalarni jalb qilish yoki gruming bilan aldash maqsadida kompyuterdan foydalanish bilan	Bu jinsiy aloqa qilishga rozilik berish yoshiga yetmagan bolani jinsiy jinoyat sodir etish uchun jalb qilish maqsadida kompyuter tizimidan foydalanish bilan bog‘liq bo‘lgan harakatlardir. Masalan, bu huquqbuzar bolalar bilan muloqot qilish uchun on-layn suhbatga kiradigan, o‘zini bola deb

bog‘liq xatti-harakatlar	ko‘rsatadigan va bolani suiiste'mol qilish maqsadida uchrashuvga taklif qilgan hollarni o‘z ichiga oladi. Bunday xatti-harakatlar "gruming" deb ataladi. Ba’zi mamlakatlar qonunlariga ko‘ra, bunday qoidalar bolalarga nisbatan jalb etish, keyinchalik uchrashuvga olib boradigan amaliy harakatlar bilan cheklangan.
Terroristik harakatlarni sodir etishda sherik bo‘lish maqsadida kompyuterdan foydalanish	Terroristik jinoyatlarda sherik bo‘lish uchun kompyuter tizimidan foydalanish bilan bog‘liq harakatlar. Terroristik jinoyatlar yoki jinoyatlarni sodir etishga undash maqsadida jamoatchilik bilan muloqot qilish uchun kompyuter tizimidan foydalanishni nazarda tutadi, bunda terroristik jinoyatlarning to‘g‘ridan-to‘g‘ri tashviqotdan qat'iy nazar, bunday harakat bir yoki bir necha terrorchilik jinoyati xavfini solsa jinoyat hisoblanadi. Shuningdek, ularning foydalanish maqsadida mablag‘lar bilan ta’minlash yoki to‘plash uchun yoki terroristik jinoyatlar yoki jinoyatlar ("terrorizmni moliyalashtirish" uchun kompyuter tizimlaridan foydalanish) uchun butunlay yoki qisman foydalanish uchun mo‘ljallanganligini bilgan holda kompyuter tizimlaridan foydalanishni o‘z ichiga oladi. Shuningdek, u terroristik jinoyatlar yoki jinoyatlarni rejalashtirish, o‘rganish, tayyorlash yoki tashkil etish uchun kompyuter tizimlaridan foydalanishni ham o‘z ichiga oladi ("terroristik jinoyatni rejalashtirish" deb nomlangan). Terroristik harakat deyilganda terrorizmga qarshi kurash bo‘yicha universal huquqiy vositalarga muvofiq belgilangan yoki qurolli mojarolar holatlarida harbiy harakatlarda faol ishtirok etmayotgan fuqaro yoki boshqa shaxsga o‘lim yoki jiddiy zarar yetkazishga qaratilgan har qanday harakat tushiniladi.

BELGILAR VA QISQARTMALAR

ACL – Access Control List
ATM - Automated teller machine
BIOS - Basic Input-Output system
CBR- Case-based reasoning
CCTV –Closed Circuit Television
CGI - Common Gateway Interface
CPU - Central Processing Unit
DAS - Directly Attached Storage
DNS - Domain Name System
DOS - Denial of Service
ICMP - Internet Control Message Protocol
IP – Internet Protocol Address
ICQ - I seek you
IOS - iPhone OS
GPS - Global Positioning System
GSM - Groupe Special Mobile
FTK - Forensic Toolkit
FTP - File Transfer Protocol
HTTP – Hyper Text Transfer Protocol
HPA – Host Protocol Area
LIR - Local Internet registry
NAS - Network Attached Storage
NIC - Network Interface Card
NGI - Next Generation Internet
ODD - Optical Disk Drive
PIN - Personal Identification Number
RAID - Redundant Array of Inexpensive Disks
RICAS - Real-time Intelligence Crime Analytics System
RIR - Regional Internet Registry
RIPE - Réseaux IP Européens (Network Coordination Centre)
TLS – Transport Layer Security
TCP – Transmission Control Protocol
URL - Uniform Resource Locator
WLAN - Wireless Local Area Network

AIJ – Avtomatlashtirilgan ish joyi
AKT – Axborot kommunikatsiya texnologiyalari

AT – Axborot texnologiyalari
DT – Dasturiy ta’minot
EHM – Elektron hisoblash mashinalari
KTE – Kompyuter-texnik ekspertiza
OT – Operatsion tizim
KIS– Katta integral sxema
RSB – Raqamli suv belgilari
RK – Ruxsatsiz kirish
ShK – Shaxsiy kompyuter
SKTE – Sud kompyuter-texnik ekspertiza
SKTE – Sud kompyuter-texnik ekspertizasi
TQT – Tezkor-qidiruv tadbirlari

TERMINLAR LUG‘ATI

ACL (Access Control List) - obyektga (dasturga, jarayonga yoki faylga) kim va nima kira olishi mumkinligini va qaysi subyektga (foydalanuvchi, foydalanuvchilar guruhi) ishlashi taqiqlangan yoki taqiqlanmaganligini belgilaydigan erkin foydalanishni boshqarish ro‘yxati.

CBR (Case Based Reasonin) – pretsedentga asoslangan fikrlash - keng ma’noda ma’lum yechimlar asosida yangi muammolarni hal qilish usuli hisoblanadi.

DAS (Directly Attached Storage) - serverlarga bevosita ulangan ma’lumotlarni saqlash tizimlari.

DNS (Domain Name System), *DNS*, domen nomlari xizmati - domen nomi tizimi, shuningdek, domen nomining rezolyutsiyasini amalga oshiruvchi server tizimi (DNS-serverlar).

DOS (DenialofService) hujum - "xizmat ko‘rsatishni rad etish" ko‘rinishidagi kompyuter tarmog‘i, kompyuter yoki axborot tizimiga hujum.

EnCase - kompyuter ekspertizasining barcha bosqichlari uchun texnologiya va dasturiy ta’minot**.**

IP-adres (Internet Protocol Address) – TCP/IP protokollar to‘plamiga asoslangan kompyuter tarmog‘idagi noyob tarmoq manzili tugunlari.

FTK (Forensic Toolkit) - kompyuter ekspertizasi sohasidagi standart.

FTP (File Transfer Protocol) – fayllarni uzatish protokoli - TCP-tarmog‘ida fayllar uzatish uchun standart protokol.

Proxy server - manzilni translyatsiya qilish deb ataladigan jarayon xavfsizlik devori bilan bog‘liq IP manzilini o‘zgartirish uchun ishlatiladigan vositachi server (xavfsizlik devori).

RAID (Redundant Array of Inexpensive Disks) - ishonchsiz komponentlardan ishonchli qurilmani hosil qilish tipik injenerlik masalasini yechimi.

Rootkit - tizimda tajovuzkor yoki zararli dastur mavjudligini izini yashiruvchi dastur yoki dasturlar majmua.

TCP (Transmission Control Protocol) – uzatishni boshqarish protokoli, Internet ma’lumotlarini uzatishning asosiy protokollaridan biri, ma’lumotlar uzatilishini boshqaradi. TCP va IP protokollariga ega tarmoqlar va quyi tarmoqlarga TCP/IP tarmoqlari deyiladi.

TLS (Transport Layer Security) – internet tarmog‘ida tugunlar orasidagi ma’lumotlarni himoyalangan holda uzatishni ta’minlaydigan transport darajasi himoya protokoli.

Wireshark - tarmoq trafigi analizatori.

Whois - domen yoki uning IP- manzili kimga qayd qilinganligi haqida server mijozga ma’lumot uzatishi mumkin bo‘lgan protokol.

Himoyaning apparat vositalari - axborotni ruxsatsiz kirish, nusxalash, o‘g‘irlash yoki o‘zgartirishdan himoya qilish uchun mo‘ljallangan mexanik, elektron, optik, lazerli, radio, radar va boshqa qurilmalar, tizimlar va tuzilmalar.

Autentifikatsiya (*Authentication*) - taqdim etilgan identifikator bo‘yicha sub’ektni kirish uchun ruxsat etilganligini tekshirish; haqiqiyligini tasdiqlash; belgilangan identifikator sifatida odatda **login** va **bank (to‘lov) karta paroli,** kartochka - mijozlar tomonidan to‘lash talab qilinganda to‘lov va boshqa hujjatlarni tuzish uchun vositalar tashkil qiladi.

Autsorsing xizmatlari (*outsourcing,outer-source-usin- tashqi manba va/yoki resurslardan foydalanish*) – buyurtmachi kompaniya qator ichki xizmatlarini va/yoki ichki servislarini, shuningdek uning dasturiy mahsulotlari, ilovalari, apparat va infrastruktura qismlaridan foydalanish asosida, tasgqi pudratchiga o‘tkazish.

Billing tizimi – hisob-kitobning avtomatlashgan tizimi.

Bot (*Boot*) - avtomatik ravishda va/yoki muntazam foydalanuvchi sifatida bir xil interfeyslar orqali biron-bir amalni oldindan belgilangan jadvalga muvofiq bajaradigan maxsus dastur.

Brandmauer *(Firewall)* - tarmoqni boshqa tizim va tarmoqlardan apparat-dasturiy vositalar nazorati yordamida, xavfsizlikka tahdidlardan himoya qilish usuli/vositasi.

Brauzer (*Brawser*), veb_brauzer, internet_brauzer, veb_klient – veb_sahifa va boshqa tarmoq axborot resurslarini ko‘rish; foydalanuvchining shaxsiy kompyuterida o‘rnatilgan, tarmoq orqali web_server bilan bog‘lanish, undan ma’lumot so‘rash va undan olish (odatda HTML formatida) uchun dastur, uni veb-sahifadagi shaklda ko‘rsatadi va qayta ishlaydi.

Virmeyker - kompyuter viruslari ishlab chiqarishchi programmist.

Virtual olam (*Virtua lreality, VR*, sun’iy borliq) - insonga sezgi organlari: ko‘riish, eshitish, hid bilish, teri sezish va boshqalar orqali texnik vositalar (obyekt va subyekt) yordamida yaratilgan dunyo.Virtual borliq ta’sir o‘tkazishni va unga javobni imitatsiya qiladi.

Veb-server - bu serverda o‘rnatilgan va HTTP yoki HTTPS protokoli yordamida **veb-sayt** bilan foydalanuvchi brauzeri o‘rtasida aloqa o‘rnatadigan dastur.

Veb-sahifa - foydalanuvchiga uzatiladigan (odatda HTML tilida) axborotning brauzerdagi natijasi**.**

Veb-sayt - "o‘rgimchak, tarmoq" va *sayt* - "joy", "joy, segment, tarmoqning bir qismi" - mantiqiy jihatdan veb-sahifalar to‘plami, jumladan server kontenti joylashuvi.

Zararli dastur, *virus*, *malware* - axborotni blokirovkalash, o‘zgartirish yoki nusxalashga olib keladigan, kompyuter, kompyuter tizimi yoki ularning tarmoqlarini buzishga sabab bo‘ladigan kompyuter dasturi. Zararli dasturlar turlari: virus, qurt, troyan, mantiqiy bomba, eksploit, rutkit.

Global navigatsiya tizimi - makon va zamon ma’lumotlarini aniqlash va uni huquqni muhofaza qilish organlari tomonidan qabul qilishni tashkil etish imkonini beruvchi usullar, dasturiy va apparat vositalar to‘plami.

Defeys - (*deface* - buzmoq, o‘zgartirmoq) - asosiy (yoki boshqa muhim) sahifa ikkinchisi bilan – odatda ko‘zga tashlanih holatida (reklama, ogohlantirish, xavf, internet) almashinishi olib keladigan xakerlik hujumi. Ko‘pincha, saytning qolgan qismiga kirish taqiqlanadi yoki eski sayt mazmuni to‘liq o‘chiriladi.

Domen - noyob domen nomi bilan belgilanadigan Internet domen nomlari ierarxik shajarasining qismi.

Qayta tiklash jurnali - ma’lumotlar bazasini yoki faylni tiklash qobiliyatini ta’minlaydigan jurnal. Bazadagi har qanday o‘zgarishlar haqida o‘rnatilgan vaqtidan buyongi ma’lumotlarni o‘z ichiga oladi, ma’lumotlar ishonchliligi va zaxira nusxasi mavjudligini ko‘rsatadi.

Tergich (*Dialers*) - pullik telefon liniyalari suiste'mol qilish orqali firibgarlik turi.

Zombi tarmog‘i, botnet - yagona markazdan boshqariladigan troyan dasturi turi bilan zazarlangan kompyuterlar guruhi; odatda, bunday tarmoq tuzilmasi keraksiz boshqarish aloqalari bilan tuzilgan; spam yuborish, hujumlar uyushtirish, trafikning haqiqiy manbalarini yashirish va boshqa vazifalarni bajarish uchun ishlatiladi; birdan o‘n minglab kompyuterlarga ega bo‘lishi mumkin.

Axborot tizimi - ma’lumotlar bazalarida va axborot texnologiyalarida va uni qayta ishlashni ta’minlaydigan texnik

vositalardagi ma’lumotlar to‘plami; axborot tizimi ko‘pincha "kompyuter, kompyuter tizimi, ularning tarmog‘i" deb atash mumkin.

Sun'iy intellekt - aqlli mashinalar, ayniqsa aqlli kompyuter dasturlari yaratishning ilm-fan va texnologiyasi; aqlli tizimlarning an’anaviy ravishda insonning imtiyozi deb hisoblangan ijodiy funksiyalarni amalga oshirish qobiliyati.

Insayder (*Insider*) - keng omma foydala olmaydigan axborotdan foydalanish imkoniga ega bir guruh odamlar a’zosi. Termin sir bilan bog‘liq bo‘lgan kontekstda yashirin, yoki biron-bir boshqa nodavlat ommaviy axborot yoki bilimga nisbatan ishlatiladi: insayder - faqat ushbu guruhda mavjud ma’lumotlarga ega guruh a’zosi.

Insident - ruxsatsiz kirishni ta’minlash yoki kompyuter tizimiga hujum qilish uchun qilingan urinish.

AT (Axborot texnologiyalari) - kompyuterlar, kompyuter dasturlari, kompyuter tarmoqlari bilan bog‘liq bilimlar va iqtisodiyotining sohasi; aloqa sohasi bilan chambarchas bog‘liq.

Karder - kartalar nusxalarini olish, tovarlar va xizmatlarni sotib olish uchun ulardan foydalanib, kartalardan ma’lumotlarni olish, ya’ni noqonuniy bank (to‘lov) kartalaridan do‘kon va bankomatlarda foydalanish bilan shug‘ullaniuvchi firbgarlik.

Karding - bank (to‘lov) kartalari katalogi bilan firibgarlik.

Kiber jinoyat - elektron sohasidagi kompyuter tizimi yoki tarmoq yordamida yoki ularga qarshi sodir etiladigan har qanday jinoyat.

Kiber jinoyatchilik - kompyuter tizimi yoki tarmog‘i orqali, shu jumladan kompyuter tizimida yoki tarmoq orqali noqonuniy egalik qilish, taklif qilish yoki tarqatish kabi jinoyatlar kabi qonunbuzar harakatlar.

Kompyuter virusi - o‘z nusxalarini yaratish imkoniga ega (original bo‘lishi shart emas) va ularni fayllar, kompyuter tizimi, kompyuter tarmoqlariga tadbiq etadigan va boshqa zararli harakatlarni bajaradigan, shu bilan birga keyinchalik tarqalish xususiyatini saqlab qoladigan dastur.

Kiberskvotting, *cybersquotting*, *skvotting*, domenni egallash - ularni keyinchalik sotish yoki nohaq foydalanish maqsadida domen nomlarini sotib olish.

Kompyuter abordaji (*haking*) - kompyuter yoki tarmoqqa huquqsiz kirish.

Kompyuter-texnik ekspertiza (KTE) – sud ekspertizasining bir turi bo‘lib, uning obyekti kompyuter texnikasi va (yoki) kompyuter ma’lumot tashish vositalari, maqsadi esa dalillarni izlash va belgilash.

Kontrafakt nusxa, *litsenziyasiz nusxa, pirat nusxa* - mualliflik huquqi va turdosh huquqlarning buzilishiga olib keladigan ishlab chiqarish yoki tarqatish ishlari (dastur, fonogramma).

Kontsentrator, *tarmoq kontsentratori, hub* - 2-bosqichda ishlaydigan freymlarni tarqalishini (takrorlashni) amalga oshiruvchi tarmoq aloqa qurilmasi, kompyuterlarni kompyuter tarmog‘ining bir qismida ulash uchun ishlatiladi; kommutatordan farqli o‘laroq, har bir olingan freym bir emas, balki barcha portlarga yuboriladi; odatda, konfiguratsiya qilinmaydi va nazorat qilinmaydi.

Log, log-fayl - kompyuterning voqea jurnali; ma’lum bir axborot tizimi yoki dasturiga ta’luqli hodisalarning yozuvlari bilan fayl yoki ma’lumotlar bazasi.

Login, *foydalanuvchi nomi* – foydalanuvchining belgili identifikatori; ko‘pincha autentifikatsiya qilish uchun parol bilan birga ishlatiladi.

Mantiqiy bomba - dasturning turi (ba’zan zararli deb tan olingan), uning maqsadi o‘rnatilgan kompyuterda eng nozik ma’lumotlarni yo‘q qilishdir; oldindan aniqlangan shartlarni bajarmagan yoki amalga oshira olmaganligi sababli paydo bo‘lgan.

Marshrutizator, *router, ruter* - (odatda IP protokoli tomonidan) paketlarni marshrutlovchi 3-darajada ishlovchi vosita, turli tarmoq qatlamlariga ulash uchun ishlatiladi.

Ruxsatsiz kirish (RK) - belgilangan tartibni buzgan holda axborot tizimiga yoki kompyuter ma’lumotlariga kirish; bu atama "noqonuniy kirish" huquqiy atamasidan farqli o‘laroq, texnik hisoblanadi, lekin deyarli bir xil ma’noni anglatadi.

Yangilanish, *patch* - alohida kompyuter dasturini yoki butun axborot tizimini funksionalligini oshirish yoki noto‘g‘ri xatolar uchun yangilash uchun mo‘ljallangan o‘rnatish ko‘rsatmalariga ega dastur yoki ma’lumotlar to‘plami; mustaqil qiymatga ega emas, faqat yangilangan dastur bilan ishlatiladi; yangilanishlar, odatda, yangilanayotgan dastur ishlab chiqarilgan kompaniya tomonidan ishlab chiqariladi, lekin ba’zan boshqa shaxslar tomonidan yaratilgan yangilanishlar ham uchrab turadi.

Tezkor-qidiruv tadbirlari (TQT) – ma’lum taktik masalalarni yechishga qaratilgan o‘zaro aloqador harakatlar tizimidan iborat operativ- qidiruv faoliyatining muhim elementi.

PIN-kod - (Personal Identification Number- shaxsiy identifikatsiya nomeri) - parol analogi. Operatsiyani avtorizatsiya qilish vaqtida u karta egasining terminalga (bankomatga) kirishi uchun parol sifatida va so‘rovni raqamli imzolash uchun maxfiy kalit sifatida ishlatiladi. PIN-kod kredit va shunga o‘xshash kartalar uchun taqdim etilgan; karta egasiga ruxsat berish uchun ishlatiladi.

Dasturiy ta’minot, DT, *software*, *soft* - EHM dasturlari uchun umumlashtirilgan nom; termin dasturiy va apparat (*yumshoq* va *qattiq*) qismlarni solishtirishda qo‘llaniladi.

Kommunikatsiya protokoli, almashinuv protokoli - turli dasturlar, qurilmalar, axborot tizimlari orasidagi ma’lumotlarni almashish qoidalari to‘plami; odatda texnik standart bilan aniqlanadi; bitta protokolning ikkita dasturiga rioya qilish ularning muvofiqligi uchun zarur shartdir.

Registratorlar - Internetda IP-manzillarni ajratish va qayd qilish bilan shug‘ullanuvchi tashkilot (IP Registry).

Referer (to refer - jo‘natmoq, yo‘naltirmoq) referal dastur doirasida daromad olish maqsadida foydalanuvchilarni ma’lum internet-resurslariga yo‘naltiruvchi odam.

Tarmoq kartasi, *tarmoq platasi, NIC* (network interface card) - muayyan interfeys orqali tarmoq bilan o‘zaro ta’sirlashuv vazifalarini bajaradigan kompyuter platasi (qurilma); Tarmoq simini yoki antennani ulash uchun bir yoki bir nechta tashqi konnektorga ega.

Skimming (*skimming*) – maxsus qurilma yordamida karta ma’lumotlarini o‘g‘irlash. Buzg‘unchilar kartaning magnit chizig‘idan barcha ma’lumotlarni ko‘chirib olishadi. Skimming PIN-kodni mini-kamera yoki katakchalar yordamida topish imkonini beradi.

Sniffer yoki *trafik analizatori* (*to sniff - hidlamoq*) - tarmoq trafigini (o‘ziniki yoki birovnikini) qo‘lga olish va tahlil qilish dasturi yoki qurilmasi.

Ijtimoiy muhandislik - axborot xavfsizligi tizimini xizmat xodimlari va foydalanuvchilar bilan aloqada olingan ma’lumotlar yordamida chetlab o‘tish, xiyla va nayranglarni qo‘llash orqali ularning ishlarini chalkashtish.

Spam – electron pochta orqali nomaqbul, ommaviy jo‘natmalar, ICQ, SMS va boshqa elektron aloqa vositalarida kamroq uchraydi

Spamer - spamni yuborish yoki spam jo‘natish (manzillarni to‘plash, jo‘natish uchun dasturlarni yaratish, spam tarqatilgan

resurslarni saqlash va boshqalar) bilan shug‘ullanadigan professional shaxs.

Steganografiya - ochiq axborot massivlarida maxfiy ma’lumotlarni yashirish uchun matematik usullarni o‘rganadigan fanning sohasi.

Trafik , *tarmoq trafigi* - raqamli aloqa liniyasi orqali uzatiladigan ma’lumotlarning miqdori bit yoki baytlarda o‘lchanadi; kamroq holatlarda atama axborot oqimini anglatadi, ya’ni bir vaqtning birligiga etkazilgan ma’lumotlarning miqdori, bit/s yoki bayt/s; tarmoq orqali uzatiladigan freymlar, paketlar, datagramlarning tarkibi.

Troyan dasturi, *trojan* - yashirincha yoki niqoblanib foydalanuvchining kompyuteridagi dasturiy ta’minotiga foydalanuvchining (operatorning) manfaatlariga va xohishiga mos bo‘lmagan xatti-harakatlarni bajarish uchun ruxsatsiz o‘rnatiladigan zararli dastur turi.

Fayl (file) - disk yoki boshqa kompyuter vositalarining nomlangan maydoni; nomi, boshqa atributlari va alohida sarlavhasi hamda alohida fayl tanasiga ega; fayl tizimida axborotni saqlash birligi hisoblanadi.

Fishing (*phishing*) - onlayn firibgarlik turi, jabrlanuvchining shaxsiy ma’lumotlarini (bank kartasi, parol, shaxsiy identifikatsiya ma’lumotlari) olishga asoslangan. Bunda xuddi ishonchli tashkilotlar (bank, provayderlar, davlat organlari) tomonidan jo‘natilgan qalbaki xat va veb-saytlardan foydalanadi.

Friker - apparat-elektron qurilmalarning himoyasini yengib o‘tish bo‘yicha mutaxassis.

Haker - juda yuqori malakali kompyuter mutaxassisi; tajovuz qiluvchi kompyuter ma’lumotlariga, odatda tarmoq orqali ruxsatsiz kirishni amalga oshiradi.

Hesh , hesh-summa yoki bir tomonlama hesh funksiyasi - maxsus algoritm yordamida fayl mazmunidan hisoblanuvchi uzun sonlar qatori. Xesh summasi checksumga o‘xshaydi, biroq u bir muhim farqga ega: bu bir tomonlama funksiyadir. Ya’ni, faylni xesh funksiyasini hisoblash oson, lekin ma’lum bir hesh funksiyasiga mos faylni tanlash mumkin emas.

Gruming - bolalarni Internetdan aldash uchun tajovuzkorlarning harakatlarini belgilaydi. Bu usul metodikaning asosiy mohiyatini anglatadigan "g‘amxo‘rlik" yoki "g‘amxo‘rlik" deb tarjima qilingan inglizcha so‘zlashtiruvchi terimdan kelib chiqadi: bolaga g‘amxo‘rlik

hissi yaratish va keyingi jinoyatlarni sodir etish uchun barqaror psixologik aloqani o‘rnatish.

Raqamli suv belgisi (RSB) – multimedia fayllarining mualliflik huquqini himoyalash dasturi. Odatda raqamli suv belgilar ko‘rinmas bo‘ladi. Biroq RSB tasvir yoki videoda ko‘rinishi mumkin. Odatda bu ma’lumot muallifni identifikatsiya qiluvchi matn yoki logotip bo‘lishi mumkin.

Ekvayring - o‘ziga bank kartochkalari orqali amalga oshiriladigan operatsiyalar bo‘yicha savdo korxonalari (xizmatlarni) bilan hisob-kitoblarni amalga oshirish va ushbu kredit tashkilotining mijozlari bo‘lmagan bank kartochkalarini egalariga naqd pul berish bo‘yicha operatsiyalarni amalga oshiradigan kredit tashkilotlari faoliyati.

Ekvayver- ekvayveringni amalga oshiradigan kredit tashkiloti.

Ekspert-kriminalist - jinoyat sodir etilgan joydan dalillarni to‘plash va tekshirish bo‘yicha mutaxassis.

Eksployt - kompyuter dasturi, dasturiy ta’minot kodining bir qismi yoki dasturiy zaifliklardan foydalanadigan va kompyuter tizimiga hujum qilish uchun ishlatiladigan buyruqlar ketma-ketligi.

Eskapizm - psixologik travmalar, murakkab ish faoliyati, xavfli yashash muhiti, “asabiy ishda” faoliyat yurutmaydigan insonlar bilan yaxshi munosabatlar o‘rnata olmaslik tufayli kelib chiqadigan doimiy va kuchli stress sababli paydo bo‘ladigan holatlarda real olamdan qochish.

MUNDARIJA

S.Y.YUSUPOV,
SH.R.GULOMOV, N.B.NASRULLAYEV

RAQAMLI KRIMINALISTIKA

(O‘quv qo‘llanma)

Toshkent – «Aloqachi» – 2020

Muharrir:	Q.Matqurbonov
Tex. muharrir:	A.Tog‘ayev
Musavvir:	B.Esanov
Musahhiha:	F.Tog‘ayeva
Kompyuterda sahifalovchi:	B.Berdimurodov

Nashr.lits. AI №176. 11.06.11.
Bosishga ruxsat etildi: 11.12.2019. Bichimi 60x841 /16.
Shartli bosma tabog‘i 15,5. Nashr bosma tabog‘i 15,0.
Adadi 100. Buyurtma № .

«Nihol print» Ok da chop etildi.
Toshkent sh., M. Ashrafiy ko‘chasi, 99/101.