B.B.MUSAEV, A.AKBAROV, Z.X.YUSUPOVA, A.M.DJURABAYEV

KIBERSPORT ASOSLARI

CHIRCHIQ 2023

O‘ZBEKISTON RESPUBLIKASI YOSHLAR SIYOSATI VA SPORT VAZIRLIGI

O‘ZBEKISTON DAVLAT JISMONIY TARBIYA VA SPORT UNIVERSITETI

B.B.MUSAEV, A.AKBAROV, Z.X.YUSUPOVA, A.M.DJURABAYEV

KIBERSPORT ASOSLARI

O‘zbekiston davlat jismoniy tarbiya va sport universiteti o‘quv-uslubiy Kengashining 2023-yil 29- martdagi 3-sonli yig‘ilish bayonnomasiga asosan uslubiy qo‘llanma sifatida nashrga tavsiya etilgan

CHIRCHIQ 2023

Mualliflar: – Musaev Baxrom Baxtiyorovich. O‘zDJTSU. Ilmiy ishlar va innovatsityalar bo‘yicha prorektor p.f.n., professor.
Akbarov Axmatjon. “Sport huquqi, ijtimoiy va tabiiy-ilmiy fanlar” kafedrasi f-m.f.n professor.
Yusupova Zebo Xusanovna. “Sport huquqi, ijtimoiy va tabiiy-ilmiy fanlar” kafedrasi p.f.b.f.d (PhD).
Djo’rabayev Avazbek Muhammadaminovich. “Sport huquqi, ijtimoiy va tabiiy-ilmiy fanlar” kafedrasi o’qituvchisi

Kibersport asoslari *uslubiy qo‘llanma//;-Ch.:“O‘zbekiston davlat jismoniy tarbiya va sport universiteti nashryoti”, 2023.-105b.*

Taqrizchilar: – **Boymurodov Adham Xushimqulovich. –** pedagogika fanlari bo`yicha falsafa doktori (PhD), Chirchiq davlat pedagogika universiteti “Informatika va axborot texnologiyalari” kafedrasi mudiri.
Yakubov Fazliddin Muhiddinovich– pedagogika fanlari bo`yicha falsafa doktori (PhD), O‘zDJTSU “Sport huquqi, ijtimoiy va tabiiy-ilmiy fanlar” kafedrasi mudiri

Uslubiy qo‘llanmada kibersport va uning asosiy tushunchalari, axborotning kriptografik himoyasi, foydalanishni nazoratlash, o’yinxavfsizligi, foydalanuvchanlikni ta’minlash usullari, dasturiy vositalar xavfsizligi, axborot xavfsizligi siyosati va risklarni boshqarish, kiberjinoyatchilik, kiberhuquq, kiberetika hamda inson faoliyati xavfsizligining nazariy va amaliy asoslari muhokama etilgan.

Uslubiy qo‘llanma sport faoliyati Sport faoliyat kibersport bakalavr ta’lim yo‘nalishlari talabalari uchun hamda jismoniy tarbiya va sport sohasida faoliyat yuritadigan professor-o‘qituvchilar, mutaxassislar uchun uslubiy qo’llanma sifatida tavsiya etiladi, hamda faoliyati axborot xavfsizligini ta’minlash bilan bog‘liq bo‘lgan mutaxassislarning keng doirasi uchun ham foydali bo‘lishi mumkin.

KIRISH

Hozirgi kunlarda biz axborotlashgan jamiyatda, ya'ni har bir sekund davomida inson orqali ulkan miqdordagi axborot oqimi o‘tib turgan jamiyatda yashab turibmiz. Bu ushbu jamiyatda yashashning hech narsa bilan almashtirib va tenglashtirib bo‘lmaydigan qo‘shimcha (qandaydir darajada foydali, lekin shuning bilan birga yetarlicha zararga ham ega bo‘lgan) samara bilan bog‘liqdir.

“Kibersport turlarini yanada rivojlantirish va keng ommalashtirishga oid qo‘shimcha chora-tadbırlar to‘g‘risida” O‘zbekiston Respublikasi Prezidentining 2022 yil 16 noyabrdagi PQ-423-sonli Qarori ijrosini ta'minlash maqsadida xavfsiz kompyuter o’yinlarni yaratish tizimlarini amalga oshirish, tahlillash va testlashni amalga oshirish yuzasidan ma'lumotlar yoritib berilgan.

Uslubiy qo’llanmaning birinchi bobida kiberxavfsizlik asoslari fani sohasining vazifalari va asosiy tushunchalari, uning qo‘llanilish sohasi hamda kiberxavfsizlikda inson omili masalalari ko‘rib chiqilgan. Kiberxavfsizlikning bilim sohalari, kiberxavfsizlik va axborot xavfsizligi tushunchalari o‘rtasidagi farq misollar asosida keltirilgan. Shuningdek, kiberjinoyatchilik, kiberhuquq va kiberetika masalalariga to‘xtalib o‘tilib, kiberjinoyatchilik uchun tayinlangan jazo turlari haqida ma’lumotlar keltirilgan.

Ikkinchi bob kiberxavfsizlikning fundamental masalalariga bag‘ishlangan, hamda kiberxavfsizlik arxitekturasi, strategiyasi va siyosatini amalga oshirish tartibi xususida ma’lumotlar keltirilgan.

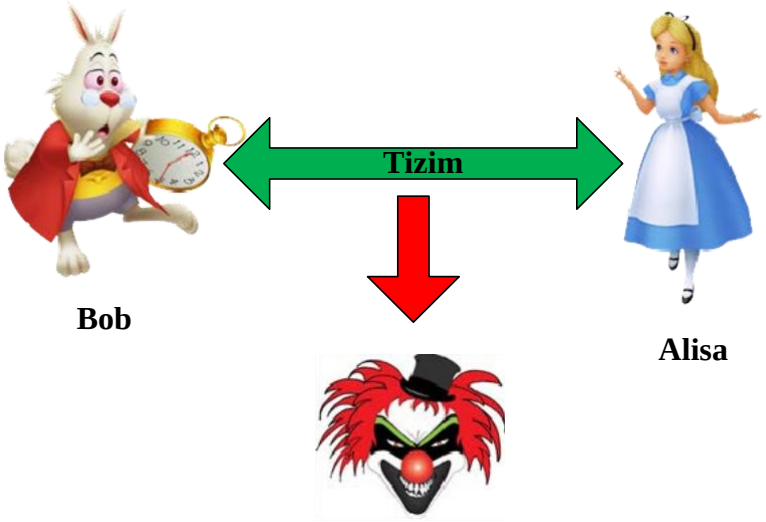
Uchinchi bobda axborotning kriptografik himoyasi doirasidagi asosiy tushunchalar, simmetrik kriptotizimlar, ochiq kalitli kriptotizimlar,ma’lumotlar yaxlitligini ta’minlash usullari, disklarni va fayllarnishifrlash hamda ma’lumotlarni xavfsiz o‘chirish usullari ko‘rib chiqilgan. Uslubiy qo’llanmaning to‘rtinchi bobi foydalanishlarninazoratlashga bag‘ishlangan bo‘lib, autentifikatsiya usullari, ma’lumotlarni fizik va mantiqiy boshqarish usullari keltirilgan. Amalda keng qo‘llanilayotgan mantiqiy foydalanishlarni boshqarish modellari va ulardan foydalanish bo‘yicha tavsiyalar bayon etilgan.

1 BOB. KIBERSPORT ASOSLARI. UMUMIY MA’LUMOTLAR

1.1Kibersportda kiberxavfsizlikning asosiy tushunchalari

Axborotni ishlash, uzatish va to‘plashning zamonaviy usullarining rivojlanishi foydalanuvchilar axborotini yo‘qolishi, buzilishi va oshkor etilishi bilan bog‘liq tahdidlarning ortishiga olib kelmoqda. Shu sababli, kompyuter tizimlari va tarmoqlarida axborot xavfsizligini ta’minlash axborot texnologiyalari rivojining yetakchi yo‘nalishlaridan biri hisoblanadi.

Axborot xavfsizligi hayotda mavjud timsollarga asoslanadi. Hayotda qonuniy faoliyat olib boruvchi shaxslar mavjud, ular 1.1-rasmda *Alisa* va *Bob* timsolida akslantirilgan. Biroq, hayotda qonuniy faoliyat yurituvchi insonlarning faoliyatiga qiziquvchi, ularning ishlariga xalaqit beruvchi insonlar ham mavjud va ular 1.1-tasvirda *Tridi* timsolida tasvirlangan. Tridi timsoli barcha g‘arazli niyatlarni amalga oshiruvchi shaxslarni ifodalaydi.



1.1-rasm. Axborot xavfsizligining hayotdagi timsollari

O‘quv uslubiy qo’llanmaning keyingi bo‘limlarini yoritishda quyidagi hayotiy senariyni ko‘raylik. Ushbu hayotiy senariy *Alisaning onlayn banki (AOB)* deb ataladi. Bunga ko‘ra, Alisa onlayn bankning biznes faoliyatini amalga oshiradi. Mazkur senariyda Alisaning xavfsizlik muammosi nima? Alisaning mijozi bo‘lgan Bobning xavfsizlik muammosichi? Alisa va Bobning xavfsizlik muammolari bir xilmi? Tridi nuqtai nazaridan qaraganda qanday xavfsizlik muammolari mavjud? Ushbu savollarga keyingi qismlarda javob berib o‘tiladi.

Kompyuter tizimlari va tarmoqlarida axborotni himoyalash va axborot xavfsizligiga tegishli bo‘lgan ayrim tushunchalar bilan tanishib chiqaylik.

Kiberxavfsizlik hozirda yangi kirib kelgan tushunchalardan biri bo‘lib, unga berilgan turlicha ta’riflar mavjud. Xususan, CSEC2017 Joint Task Force manbasida kiberxavfsizlikka quyidagicha ta’rif berilgan: *kiberxavfsizlik – hisoblashlarga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni to‘g‘ri bajarilishini kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonlarni mujassamlashtiradi. U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlillash va testlashni o‘z ichiga oladi. Kiberxavfsizlik ta’limning mujassamlashgan bilim sohasi bo‘lib, qonuniy jihatlarni, siyosatni, inson omilini, etika va risklarni boshqarishni o‘z ichiga oladi.*

Tarmoq sohasida faoliyat yuritayotgan *Cisco* tashkiloti esa kiberxavfsizlikka quyidagicha ta’rif bergan: *Kiberxavfsizlik – tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberxujumlar odatda maxfiy axborotni boshqarishni, almashtirishni yoki yo‘q qilishni; foydalanuvchilardan pul undirishni; normal ish faoliyatini buzishni maqsad qiladi. Hozirda samarali kiberxavfsizlik choralarini amalga oshirish insonlarga qaraganda qurilmalar va ularning turlari sonining kattaligi va buzg‘unchilar salohiyatini ortishi natijasida amaliy tomondan murakkablashib bormoqda.*

Kiberxavfsizlik bilim sohasining zaruriyati birinchi meynfreym kompyuterlar ishlab chiqarilganidan boshlab paydo bo‘la boshlagan. Bunda mazkur qurilmalarning va ularning vazifalarining himoyasi uchun ko‘p sathli xavfsizlik choralari amalga oshirilgan. Milliy xavfsizlikni ta’minlash zaruriyatini oshib borishi kompleks va texnologik murakkab ishonchli xavfsizlik choralarini paydo bo‘lishiga sabab bo‘ladi.

Hozirda axborot texnologiyalari sohasida faoliyat yuritayotgan har bir mutaxassisning kiberxavfsizlikning fundamental bilimlariga ega bo‘lishi talab etiladi. Kiberxavfsizlik fani sohasining tuzilishini quyidagicha tasvirlash mumkin (1.2-rasm).

1.2 – rasm. Kiberxavfsizlik fani sohasining tuzilishi

Kiberxavfsizlikni fundamental atamalarini aniqlashda turli yondashuvlar mavjud. Xususan, CSEC2017 JTF manbasida kiberxavfsizlikning quyidagi 6 ta atamasi keltirilgan:

Konfidensiallik – axborot yoki uni eltuvchisining shunday holatiki, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo‘ladi. Konfidensiallik axborotni ruxsatsiz “o‘qish”dan himoyalash bilan shug‘ullanadi. AOB senariysida Bob uchun konfidensiallik juda muhim. Ya’ni, Bob o‘z balansida qancha pul borligini Tridining bilishini istamaydi. Shu sababli Bob uchun balans xususidagi ma’lumotlarning konfidensialligini ta’minlash muhim hisoblanadi.

Yaxlitlik - axborotning buzilmagan ko‘rinishida (axborotning qandaydir qayd etilgan holatiga nisbatan o‘zgarmagan shaklda) mavjud bo‘lishi ifodalangan xususiyati. Yaxlitlik axborotni ruxsatsiz “yozish”dan (ya’ni, axborotni o‘zgartirishdan) himoyalash yoki kamida o‘zgartirilganligini aniqlash bilan shug‘ullanadi. AOB senariysida Alisaning banki qayd yozuvining yaxlitligini Tridan himoyalash shart. Masalan, Bob o‘zining akkauntida balansning o‘zgarishidan yoki Alisa akkauntida balansning oshishidan himoyalashi shart.

Shu o‘rinda konfidensiallik va yaxlitlik bir xil tushuncha emasligiga e’tibor berish kerak. Masalan, Tridi biror ma’lumotni o‘qiy olmagan taqdirda ham uni sezilmaydigan darajada o‘zgartirishi mumkin.

Foydalanuvchanlik - avtorizatsiyalangan mantiqiy obyekt so‘rovi bo‘yicha axborotning tayyorlik va foydalanuvchanlik holatida bo‘lishi xususiyati. Foydalanuvchanlik axborotni (yoki tizimni) ruxsatsiz “bajarmaslik”dan himoyalash bilan shug‘ullanadi. AOB senariysida AOB web saytidan Bobning foydalana olmasligi Alisaning banki va Bob uchun foydalanuvchanlik muammosi hisoblanadi. Sababi, mazkur holda Alisa pul o‘tkazmalaridan daromad ola olmaydi va Bob esa o‘z biznesiniamalga oshira olmaydi. Foydalanuvchanlikni buzishga qaratilgan hujumlardan eng keng tarqalgani – xizmat ko‘rsatishdan voz kechishga undovchi hujum (Denial of service, DOS).

Risk – potensial foyda yoki zarar bo‘lib, umumiy holda har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo‘shilganida risk paydo bo‘ladi. ISO “*risk* – bu noaniqlikning maqsadlarga ta’siri” sifatida ta’rif bergan.

Masalan, universitetga o‘qishga kirish jarayonini ko‘raylik. Umumiy holda bu jarayonni o‘zi risk hisoblanmaydi. Faqatgina abituriyent hujjatlarini va kirish imtihonlarini topshirganida, u o‘qishga kirishi yoki kira olmasligi mumkin. Bu o‘z navbatida qabul qilinish yoki qabul qilinmaslik riskini yuzaga kelishiga sabab bo‘ladi.

Kiberxavfsizlikda yoki axborot xavfsizligida risklarga salbiy ko‘rinishda qaraladi.

Hujumchi kabi fikrlash - bo‘lishi mumkin bo‘lgan xavfni oldini olish maqsadida qonuniy foydalanuvchining hujumchi kabi fikrlash jarayoni.

Tizimli fikrlash - kafolatlangan amallarni ta’minlash uchun ijtimoiy va texnik cheklovlarning o‘zaro ta’sirini hisobga oladigan fikrlash jarayoni.

Bundan tashqari quyidagi tushunchalar ham kiberxavfsizlik sohasini o‘rganishda muhim hisoblanadi.

Axborot xavfsizligi - axborotning holati bo‘lib, unga binoan axborotga tasodifan yoki atayin ruxsatsiz ta’sir etishga yoki ruxsatsiz undan foydalanishga yo‘l qo‘yilmaydi. Yoki, axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta’minlovchi axborotning himoyalanish darajasi holati.

Axborotni himoyalash – axborot xavfsizligini ta’minlashga yo‘naltirilgan choralar kompleksi. Amalda axborotni himoyalash deganda ma’lumotlarni kiritish, saqlash, ishlash va uzatishda uning yaxlitligini, foydalanuvchanligini va agar, kerak bo‘lsa, axborot va resurslarning konfidensialligini madadlash tushuniladi.

Aktiv - himoyalanuvchi axborot yoki resurslar. Yoki, tashkilot uchun qimmatli barcha narsalar.

Tahdid – tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. Yoki, tahdid - axborot xavfsizligini buzuvchi potensial yoki real mavjud xavfni tug‘diruvchi sharoit va omillar majmui. Tahdid o’yinchining aktivlariga qaratilgan bo‘ladi. Masalan, aktiv sifatida korxonaga tegishli biror bir saqlanuvchi hujjat bo‘lsa, u holda ushbu hujjat saqlanadigan xonaga nisbatan tahdid amalga oshirilish mumkin.

Zaiflik – bir yoki bir nechta tahdidlarni amalga oshirishga imkon beruvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik.

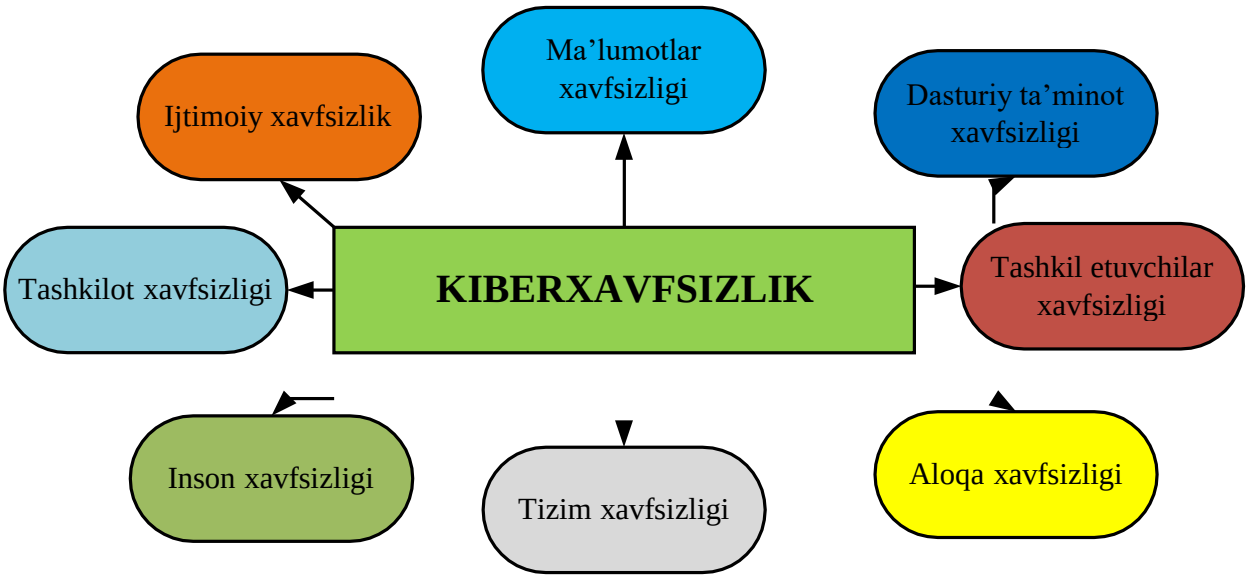
Boshqarish vositasi – riskni o‘zgartiradigan harakatlar bo‘lib, natijasi zaiflik yoki tahdidlarni o‘zgarishiga ta’sir qiladi. Bundan tashqari, boshqarish vositasining o‘zi turli tahdidlar foydalanishi mumkin bo‘lgan zaiflikka ega bo‘lishi mumkin. Masalan, tashkilotda saqlanayotgan qog‘oz ko‘rinishidagi axborotni yong‘indan himoyalash uchun o‘chirish vositalari boshqarish vositasi sifatida ko‘rilishi mumkin. Yong‘in bo‘lganida xodimlarning xatti-xarakatlari va yong‘inni oldini olish bo‘yicha ko‘rilgan chora-tadbirlar ham boshqarish vositasi hisoblanishi mumkin. Yong‘inga qarshi kurashish tizimining ishlamay qolish holatiga esa boshqarish vositasidagi kamchilik sifatida qaraladi.

Axborot xavfsizligi va kiberxavfsizlik o‘rtasidagi farq. “Kiberxavfsizlik” va “axborot xavfsizligi” atamalaridan, ko‘pincha o‘rnilari almashgan holda, foydalanishadi. Ba’zilar kiberxavfsizlikka axborot xavfsizligi, axborot texnologiyalari xavfsizligi va (axborot) risklarni boshqarish tushunchalariga sinonim sifatida qarashsa, ayrimlar esa, xususan hukumat sohasidagilar, kompyuter jinoyatchiligi va muhim infrastrukturalar himoyasini o‘z ichiga olgan milliy xavfsizlik bilan bog‘liq texnik tushuncha sifatida qaraydilar. Turli soha xodimlari tomonidan o‘z maqsadlariga moslashtirish holatlari mavjud bo‘lsada, axborot xavfsizligi va kiberxavfsizlik tushunchalari orasida ba’zi muhim farqlar mavjud.

Axborot xavfsizligi sohasi, axborotning ifodalanishidan qat’iy nazar (qog‘oz ko‘rinishidagi, elektron va insonlar fikrlashida, og‘zaki va vizual) intelektual huquqlarni himoyalash bilan shug‘ullanadi. *Kiberxavfsizlik* esa elektron shakldagi axborotni (barcha holatdagi, tarmoqdan to qurilmagacha bo‘lgan, o‘zaro birga ishlovchi tizimlarda saqlanayotgan, uzatilayotgan va ishlanayotgan axborotni) himoyalash bilan shug‘ullanadi. Bundan tashqari, hukumatlar tomonidanmoliyalashtirilgan hujumlar va rivojlangan doimiy tahidlar (Advanced

persistent threats, APT) ham aynan kiberxavfsizlikka tegishli. Qisqacha aytganda, kiberxavfsizlikni axborot xavfsizligining bir yo‘nalishi deb tushunish uni to‘g‘ri anglashga yordam beradi.

Kiberxavfsizlikning bilim sohalari. CSEC2017 JTF manbasiga ko‘ra kiberxavfsizlik 8 ta bilim sohasiga bo‘lingan, o‘z o‘rnida ularning har biri qismsohalarga bo‘linadi (1.3-rasm).



1.3-rasm. Kiberxavfsizlikning bilim sohalari

“*Ma’lumotlar xavfsizligi*” bilim sohasining maqsadi ma’lumotlarni saqlash, ishlash va uzatishda himoyani ta’minlash. Mazkur bilim sohasida himoyani to‘liq amalga oshirish uchun matematik va analitik algoritmlardan foydalaniladi.

“*Dasturiy ta’minot xavfsizligi*” bilim sohasi foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy vositalarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi.

“*Tashkil etuvchilar xavfsizligi*” bilim sohasi katta tizimlarda integrallashgan tashkil etuvchilarni loyihalashga, sotib olishga, testlashga, tahlillashga va texnik xizmat ko‘rsatishga e’tibor qaratadi. Tizim xavfsizligi gohida tashkil etuvchilar xavfsizligidan farq qiladi. Tashkil etuvchilar xavfsizligi tizimning qanday loyihalanganligiga, yaratilganligiga, sotib olinganligiga, boshqa tarkibiy qismlar bilan bog‘langanligiga, qanday ishlayotganligiga va saqlanayotganligiga bog‘liq bo‘ladi.

“*Aloqa xavfsizligi*” bilim sohasi tashkil etuvchilar o‘rtasidagi aloqani himoyalashga e’tibor qaratib, o‘zida fizik va mantiqiy ulanishni mujassamlashtiradi.

“*Tizim xavfsizligi*” bilim sohasi tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat tizim xavfsizligining jihatlariga e’tibor qaratadi. Tizim xavfsizligini tushunish uchun, nafaqat uning tarkibiy qismlari va ularning bog‘lanishlarini tushunish, balki yaxlitlikni ham hisobga olish talab etiladi. Ya’ni, tizimni to‘liqligicha ko‘rib chiqish talab etiladi. Mazkur bilim sohasi, “Tashkil etuvchilar xavfsizligi” va “Aloqa xavfsizligi” bilim sohalari bilan bir qatorda, tashkil etuvchilar bog‘lanishlarining xavfsizligi va undan yuqori tizimlarda foydalanish masalasini hal etadi.

“*Inson faoliyati xavfsizligi*” bilim sohasi kiberxavfsizlik bilan bog‘liq inson hatti-harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida ma’lumotlarni va shaxsiylikni himoya qilishga e’tibor qaratadi.

“*Tashkilot xavfsizligi*” bilim sohasi tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini madadlash uchun risklarni boshqarishga e’tibor qaratadi.

“*Ijtimoiy xavfsizlik*” bilim sohasi jamiyatda u yoki bu darajadagi ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi. Kiberjinoyatchilik, qonunlar, axloqiy munosabatlar, siyosat, shaxsiy hayot va ularning bir-biri bilan munosabatlari ushbu bilim sohasidagi asosiy tushunchalar hisoblanadi.

Demak, aytish mumkinki, kiberxavfsizlik sohasi axborot texnologiyalari mutaxassislari uchun zarur soha hisoblanadi.

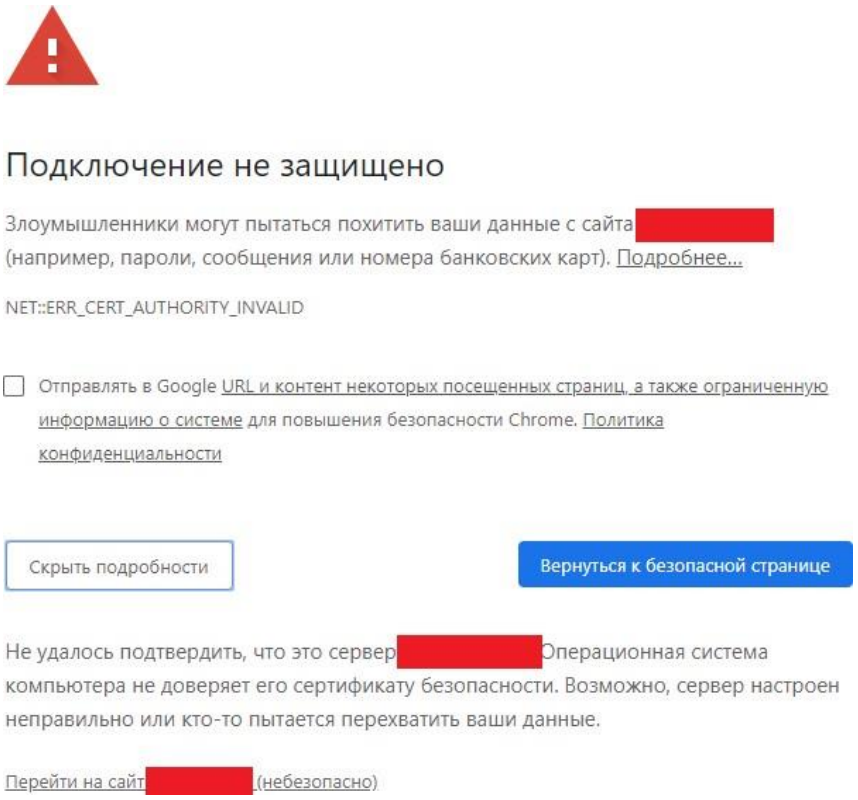
1.1. Kiberxavfsizlikda inson omili

Foydalanuvchilarga kiberxavfsizlik tizimidagi eng zaif nuqta sifatida qaraladi. Foydalanuvchilar tomonidan har qanday yuqori darajadagi xavfsizlik ham buzilishi mumkin. Masalan, Bob amazon.com onlayn do‘konidan biror narsani sotib olmoqchi, deylik. Buning uchun Bob turli kriptografik usullarga tayanadigan SSL (Secure Sockets Layer) protokoli yordamida Amazon bilan ishonchli bog‘lanish uchun web-brauzerdan foydalanishi mumkin. Ushbu protokol barcha zarur amallar to‘g‘ri bajarilganida kafolatli xavfsizlikni ta’minlaydi. Biroq, ushbu protokolga qaratilgan ba’zi hujum turlari (O‘rtada turgan odam hujumi, Man-in-the-middle attack) mavjudki, ularning amalga oshishi uchun foydalanuvchi “ishtiroki” talab etiladi (1.4-rasm). Agar foydalanuvchi

xavfsiz holatni tanlasa (*Вернуться к безопасной странице*) hujum amalga oshmaydi. Biroq, foydalanuvchi tomonidan xavfsiz bo‘lmagan tanlov (*Перейти на сайт .... (небезопасно)*) amalga oshirilganida hujum muvaffaqiyatli tugaydi. Boshqacha aytganda, yuqori xavfsizlik darajasiga ega protokoldan foydalanilganda ham foydalanuvchining noto‘g‘ri harakati sababli xavfsizlik buzilishi mumkin.

Odatda foydalanuvchilar esda saqlash oson bo‘lgan parollardan foydalanishga harakat qiladilar. Biroq, bunday yo‘l tutish buzg‘unchi uchun parollarni taxminlab topish imkoniyatini oshiradi. Boshqa tomondan, murakkab parollardan foydalanish va ularni turli eltuvchilarda saqlash (masalan, qog‘ozda qayd etish) esa, ushbu muammoni yanada kuchaytiradi.

Bu misollar inson omili tufayli turli joylar va holatlarda xavfsizlik muammolarining kelib chiqishi mumkinligini ko‘rsatadi. Inson omili tufayli yuzaga keladigan xavfsizlik muammolariga ko‘plab misollar keltirish mumkin. Biroq, keltirilgan holatlardagi eng muhim jihat shundaki, xavfsizlik nuqtai nazaridan “tenglamadan” inson omilini olib tashlash zarur. Boshqacha aytganda, inson omili ishtirok etmagan tizimlar ishtirok etgan tizimlarga nisbatan xavfsizroq bo‘ladi.



1.4-rasm. SSL protokolidagi xavfsizlik ogohlantirishi

Eng muhim inson omillariga quyidagilar taalluqli:

– *Kiberxavfsizlik sohasiga oid bilimlarni yetishmasligi* katta hajmdagi oshkor zaifliklarni paydo bo‘lishiga olib keladi. Kiberxavfsizlik sohasi an’anaviy xavfsizlikka aloqador bo‘lgani bois, zarur texnologik moslashishning tezkorligi ko‘p hollarda bo‘lishi mumkin bo‘lgan zaifliklar sonini oshiradi. Boshqa tomondan, insonning sohaga tegishli so‘nggi texnologik bilimlarni o‘zlashtirishi har doim ham yetarli bo‘lmaydi.

– *Risklarni bartaraf etishni va ular haqida xabar berishning yetarli bo‘lmasligi* kiberxavfsizlikda takrorlanuvchi va kutilmagan buzilishlarga sababchi bo‘ladi. Insonlar odatda tashkilotlariga jiddiy xavf soluvchi risk mavjudligini bilishsada, uni oshkor qilishmaydi. Buning asosiy sababi sifatida risk bevosita shaxsning o‘ziga, uni moliyaviy holatiga ta’sir etmasligini yoki oshkor qilinganida shaxsning obro‘si tushishini keltirishadi.

– *Madaniyat va munosabatlardagi muammolarga* o’yinchining o‘zi yoki tashkilot ichki ma’lumotlarini biluvchi norozi va e’tiborsiz xodimning paydo bo‘lishi sababchi bo‘lishi mumkin. Kiberxavfsizlik muammolarining aksariyati ichki hisoblanib, ular xodimlar orasidagi turli kelishmovchiliklar va tashkilot ichidagi muhitning yaxshi emasligi natijasida yuzaga keladi. Bu sabablar esa, xodimning tashkilot ichki strukturasini yaxshi bilgani bois, aksariyat hollarda jiddiy muammolarga olib keladi.

– *Xavfsizlik mashg‘ulotlariga kam mablag‘ sarflanishi* boshqarilayotgan xavfsizlik risklari to‘g‘risidagi ma’lumotning kamligi sababchi bo‘ladi. Odatda, soha korxonalaridagi xodimlar mustaqil ravishda kiberxavfsizlik qoidalarini o‘rganishmaydi. Shuning uchun kiberxavfsizlik qoidalarini xodimlarga maxsus mashg‘ulotlar shaklida yetkazish zarur bo‘ladi. Bu esa tashkilotdan xavfsizlik mashg‘ulotlariga yetarlicha mablag‘ sarflanishni talab qiladi.

– *Hisobga olish nuqtasining yagona emasligi* natijasida xavfsizlikning to‘laqonli amalga oshirilmasligi kuzatiladi. Amalda xavfsizlikni kafolatli ta’minlashda uning nazoratini bir nuqtada amalga oshirish muhim hisoblanadi. Yagona nuqtada amalga oshirilgan xavfsizlik nazorati taqsimlangan shakliga nisbatan ishonchli bo‘ladi. Biroq, tashkilotlardagi xavfsizlik nazoratining murakkabligi bois, nazorat odatda taqsimlangan holda boshqariladi.

– *Ijtimoiy injineriya* asosida xavfsizlik nazoratini aylanib o‘tishda foydalanuvchidan, an’anaviy josuslik texnikasi yordamida, ma’lumotlar qo‘lga kiritiladi. Eng yaxshi kiberxavfsizlik tizimiga ega bo‘lgan tashkilotga ham ijtimoiy injineriya tahdidi xavf solishi mumkin. Ayniqsa, foydalanuvchilarni turli ijtimoiy tarmoqlarda shaxsiy ma’lumotlarini e’tiborsizlik bilan qoldirishi bu xavfning keskin ortishiga sababchi bo‘lmoqda.

1.2. Kiberjinoyatchilik, kiberqonunlar va kiberetika

Kiberjinoyatchilik – g‘arazli yoki xuliganlik maqsadlarida himoyalashning kompyuter tizimlarini buzib ochishga, axborotni o‘g‘irlashga yoki buzishga yo‘naltirilgan alohida shaxslarning yoki guruhlarning harakatlari.

Kiberhujumga duch kelgan tashkilot uchun kiberjinoyatlar ichki yoki tashqi bo‘lishi mumkin:

Ichki kiberjinoyatlar: tarmoqqa yoki kompyuter tizimiga, ular bilan tanish va ulardan qonuniy foydalanish huquqiga ega bo‘lgan shaxs tomonidan, amalga oshiriladi. Mazkur turdagi kiberjinoyatlar odatda o’yinchining xafa bo‘lgan va norozi xodimlari tomonidan amalga oshiriladi. Ushbu xodimlarning maqsadi esa tashkilot yoki uning rahbaridan o‘ch olish yoki ochko‘zlik bo‘lishi mumkin. Xafa bo‘lgan xodim, AT infrastrukturasi, xavfsizlik arxitekturasi va tizimi bilan yaqindan tanish bo‘lgani bois, mazkur turdagi jinoyatchilik tashkilotga jiddiy ziyon yetkazishi mumkin. Bundan tashqari, kiberjinoyatchi tashkilot tarmog‘idan foydalanish imkoniyatiga ega bo‘ladi. Shuning uchun, ichki kiberjinoyatchilik natijasida maxfiy axborotning sirqib chiqish imkoniyati yuqori bo‘ladi.

Tashqi kiberjinoyatlar: odatda tashqaridan yoki tashkilot ichkarisidan yollangan hujumchi tomonidan amalga oshiriladi. Mazkur kiberjinoyatchilik o’yinchining nafaqat moliyaviy yo‘qotishlariga, balki obro‘sining yo‘qolishiga ham sababchi bo‘ladi. Hujum tashqaridan amalga oshirilgani bois, hujumchi harakatni tashkilot AT infrastrukturasini skaner qilish va unga aloqador ma’lumotlarni to‘plashdan boshlaydi. Xususan, malakali buzg‘unchi dastlab tashkilotda foydalanilgan tarmoqlararo ekran vositasining log faylini tahlil qilishdan boshlaydi. Shu bois, tarmoq ma’muri mazkur imkoniyatni buzg‘unchiga taqdim etmasligi shart.

Kiberjinoyat amalga oshirilganida quyidagilar asosiy maqsad sifatida qaraladi:

– mablag‘, qimmatli qog‘ozlar, kredit, moddiy boyliklar, tovarlar, xizmatlar, imtiyozlar, ko‘chmas mulk, yoqilg‘i xom ashyosi, energiya manbalari va strategik xom ashyolarni noqonuniy o‘zlashtirish;

– soliq va boshqa yig‘imlarni to‘lashdan bosh tortish;

– jinoiy daromadlarni qonunlashtirish;

– qalbaki hujjatlar, shtamplar, muhrlar, blankalar, shaxsiy yutuq chiptalarini qalbakilashtirish;

– shaxsiy yoki siyosiy maqsadlarda maxfiy ma’lumotlarni olish;

– ma’muriyatning yoki ishdagi hamkasblarning g‘arazli munosabatlari uchun qasos olish;

– shaxsiy yoki siyosiy maqsadlar uchun mamlakat pul tizimini buzish;

– mamlakatdagi vaziyatni, hududiy ma’muriy tuzilishni beqarorlashtirish;

– talonchilik, raqibni yo‘q qilish yoki siyosiy maqsadlar uchun muassasa, korxona yoki tizim ish tartibini buzish;

– shaxsiy intelektual qobiliyatini yoki ustunligini namoyish qilish.

Kiberjinoyat turlarini qat’iy tasniflashning imkoni yo‘q. Quyida kriminologiya sohasiga nisbatan kiberjinoyatlarning turlari keltirilgan:

– iqtisodiy kompyuter jinoyatchiligi;

– inson va fuqarolarning konstitutsiyaviy huquqlari va erkinliklariga qarshi qaratilgan kompyuter jinoyatchiligi;

– jamoat va davlat xavfsizligiga qarshi kompyuter jinoyatchiligi.

Iqtisodiy kompyuter jinoyatchiligi amalda ko‘p uchraydi. Ular jinoyatchilarga millionlab AQSh dollari miqdoridagi noqonuniy daromadlar keltiradi. Ular orasida keng tarqalgani firibgarlik, asosan, bank hisob raqamlari va bank kartalari orqali amalga oshiriladi. Xalqaro amaliyotda plastik kartalar bilan sodir etilgan jinoyatlar yo‘qolgan yoki o‘g‘irlangan kartalar, soxta to‘lov kartalarini yaratish yoki ulardan foydalanish, karta taqdim etmasdan bank hisob varag‘i ma’lumotlarini olish va noqonuniy foydalanish, shuningdek, karta egasi tomonidan sodir etilgan jinoyatlar bilan bog‘liq.

Kiberjinoyatlarning yana bir turi inson va fuqorolarning huquqlariga va erkinliklariga qaratilgan jinoyatlar - “kompyuter qaroqchiligi”dir. Ushbu jinoyatlar dasturiy ta’minotni noqonuniy nusxalash, ishlatish va tarqatishda namoyon bo‘ladi. Bu dasturiy ta’minot va ma’lumotlar bazasini yaratish bilan bog‘liq huquqiy munosabatlarga

(mualliflik huquqiga) jiddiy zarar yetkazadi. Bundan tashqari, dasturiy ta’minot kompaniyalariga katta moliyaviy yo‘qotishlarni olib keladi.

“Maykrosoft Armaniston” kompaniyasining direktori Grigor Barsegyanning ta’kidlashicha, “kompyuter qaroqchiligi”ning ishlab chiqaruvchilarga yetkazgan zarari yiliga 66 milliard dollarni tashkil etgan. Uning so‘zlariga ko‘ra Armanistonlik iste’molchilar, o‘zlarining moliyaviy resurslarini tejash maqsadida, viruslarni yuqtirish xavfi yuqori bo‘lgan dasturlardan ongli ravishda foydalanganlar.

Kompyuter jinoyatchiligining oxirgi turi - jamoat yoki davlat xavfsizligiga qarshi kompyuter jinoyatchiligi, ularga davlat yoki jamoat xavfsizligiga qaratilgan xavfli xatti - harakatlar taalluqli. Ular ko‘pincha ma’lumot uzatish qoidalarining, mamlakat mudofaa tizimining yoki uning tarkibiy qismlarining buzilishi bilan bog‘liq.

Kiberqonunlar. Qonun (huquq) — inson, jamiyat va davlat manfaatlari nuqtai nazaridan eng muhim hisoblanadigan ijtimoiy munosabatlarni mustahkamlash, rivojlantirish va tartibga solish vositasi. Qonunning nima maqsadga qaratilganini u yo‘naltirilgan munosabatga qarab aniqlash mumkin. Shu bois qonunlar turli sohaga oid maqsadlarga ega bo‘lishi mumkin. Umumiy nomda kiberjinoatchilikni tartibga solishni maqsad qilgan qonunlar kiberqonunlar deb ataladi.

Qonunni ishlab chiquvchilar va uni himoya qiluvchilar butun dunyo bo‘ylab kiberjinoyatchilikni aniq belgilaydigan va kiber dalillarni qabul qilishni to‘liq madadlovchi kiberqonunlar zarurligi haqida ogohlantirib keladilar. Mamlakatning biror xalqaro shartnomadagi ishtiroki bu shartnomani qonuniylashtiradigan ichki qonunlar ishlab chiqilgan va tasdiqlangan taqdirdagina kuchga kiradi. Masalan, Yevropada 2004 yilda Yevropa Kengashi butun dunyo mamlakatlariga taklif qilingan Kiberjinoyatchilik to‘g‘risidagi Shartnoma (Budapesht konvensiyasi deb ham ataladi) loyihasini qabul qildi. Mazkur Shartnomani ko‘pchilik davlatlar imzolagan bo‘lsada, ularning bir nechtasigina shartnomaga mos keladigan milliy qonunlarga ega.

2020 yil fevral oyiga kelib, Birlashgan millatlar tashkilotiga a’zo bo‘lgan 106 ta (yoki 55%) davlatlar Budapesht konvensiyasiga muvofiq milliy kiberjinoyatchilik to‘g‘risidagi qonunlarga ega bo‘ldilar. Bundan tashqari, hozirda rivojlanayotgan davlatlar kiberjinoyatchilarni tergov qilish va bu jarayon uchun kerakli ma’lumotlarni yig‘ish bo‘yicha ma’lum vakolatlarni qabul qildilar.

Xususan, Respublikamizda ham “Ilm, ma’rifat va raqamli iqtisodiyotni rivojlantirish yili”da amalga oshirishga oid davlat dasturi

to‘g‘risida”gi O‘zbekiston Respublikasi Prezidenti Farmoni loyihasi va 2020 yil Davlat dasturi loyihasida 2020–2023 yillarga mo‘ljallangan kiberxavfsizlikka doir milliy strategiya va “Kiberxavfsizlik to‘g‘risida”gi qonun loyihasi ishlab chiqish rejalashtirilgan.

Hujjatga asosan xavfsizlikni, millatlararo totuvlik va diniy bag‘rikenglikni ta’minlash, shuningdek, tashqi siyosat sohasida:

– 2020 yil 1 sentyabrga qadar kiberxavfsizlikning huquqiy asoslarini shakllantirish bo‘yicha choralar ko‘riladi, shu jumladan 2020–2023 yillarga mo‘ljallangan kiberxavfsizlikka doir milliy strategiya va “Kiberxavfsizlik to‘g‘risida”gi qonun loyihasi ishlab chiqiladi;

Loyihada:

– axborot kommunikatsiya texnologiyalari tizimini zamonaviy kibertahdidlardan himoya qilish, turli darajadagi tizimlar uchun kiberxavfsizlik bo‘yicha zamonaviy mexanizmlarni joriy etish;

– kiberxavfsizlikni ta’minlash sohasida davlat organlari,korxona va tashkilotlarning huquqlari va majburiyatlarini belgilash, ularning faoliyatini muvofiqlashtirish;

– ushbu sohadagi normativ-huquqiy hujjatlarni unifikatsiyalash nazarda tutiladi.

Kiberqonunlar har bir davlatning milliy qonun me’yorlari asosida shakllantiriladi yoki ularning bir qismini tashkil qiladi. Quyida Respublikamizdagi qonun hujjatlarida kiberjinoyatni oldini olish va tartibga solishga aloqador bo‘lgan bandlar keltirilgan.

Milliy qonunlar. 2002 yil 12 dekabrda O‘zbekiston Respublikasining 439-II – sonli “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonuni qabul qilindi. Ushbu qonun 16 moddadan iborat bo‘lib, unda xususan, quyidagilar belgilangan:

1-modda. Ushbu Qonunning asosiy vazifalari

Ushbu Qonunning asosiy vazifalari axborot erkinligi prinsiplari va kafolatlariga rioya etilishini, har kimning axborotni erkin va moneliksiz izlash, olish, tekshirish, tarqatish, foydalanish va saqlash huquqlari ro‘yobga chiqarilishini, shuningdek axborotning muhofaza qilinishini hamda shaxs, jamiyat va davlatning axborot borasidagi xavfsizligini ta’minlashdan iborat.

4-modda. Axborot erkinligi

O‘zbekiston Respublikasining Konstitutsiyasiga muvofiq har kim axborotni moneliksiz izlash, olish, tekshirish, tarqatish, undan foydalanish va uni saqlash huquqiga ega.

Axborot olish faqat qonunga muvofiq hamda inson huquq va erkinliklari, konstitutsiyaviy tuzum asoslari, jamiyatning axloqiy qadriyatlari, mamlakatning ma’naviy, madaniy va ilmiy salohiyatini muhofaza qilish, xavfsizligini ta’minlash maqsadida cheklanishi mumkin.

6-modda. Axborotning ochiqligi va oshkoraligi

Axborot ochiq va oshkora bo‘lishi kerak, maxfiy axborot bundan mustasno.

Maxfiy axborotga quyidagilar kirmaydi:

fuqarolarning huquq va erkinliklari, ularni ro‘yobga chiqarish tartibi to‘g‘risidagi, shuningdek davlat hokimiyati va boshqaruv organlari, fuqarolarning o‘zini o‘zi boshqarish organlari, jamoat birlashmalari va boshqa nodavlat notijorat tashkilotlarining huquqiy maqomini belgilovchi qonun hujjatlari;

ekologik, meteorologik, demografik, sanitariya-epidemiologik, favqulodda vaziyatlar to‘g‘risidagi ma’lumotlar hamda aholining, aholi punktlarining, ishlab chiqarish obyektlari va kommunikatsiyalarning xavfsizligini ta’minlash uchun zarur bo‘lgan boshqa axborotlar;

axborot-kutubxona muassasalarining, arxivlarning, idoraviy arxivlarning va O‘zbekiston Respublikasi hududida faoliyat ko‘rsatayotgan yuridik shaxslarga tegishli axborot tizimlarining ochiq fondlaridagi mavjud ma’lumotlar.

Davlat hokimiyati va boshqaruv organlari, fuqarolarning o‘zini o‘zi boshqarish organlari, jamoat birlashmalari va boshqa nodavlat notijorat tashkilotlari jamiyat manfaatlariga taalluqli voqealar, faktlar, hodisalar va jarayonlar to‘g‘risida qonun hujjatlarida belgilangan tartibda ommaviy axborot vositalariga xabar berishi shart.

10- modda. Axborot berishni rad etish

Agar so‘ralayotgan axborot maxfiy bo‘lsa yoki uni oshkor etish natijasida shaxsning huquqlari va qonuniy manfaatlariga, jamiyat va davlat manfaatlariga zarar yetishi mumkin bo‘lsa, axborotni berish rad etilishi mumkin.

So‘ralayotgan axborotni berish rad etilganligi to‘g‘risidagi xabar so‘rov bilan murojaat etgan shaxsga so‘rov olingan sanadan e’tiboran besh kunlik muddat ichida yuboriladi.

Rad etish to‘g‘risidagi xabarda so‘ralayotgan axborotni berish mumkin emasligi sababi ko‘rsatilishi kerak.

Maxfiy axborot mulkdori, egasi axborotni so‘rayotgan shaxslarni bu axborotni olishning amaldagi cheklovlari to‘g‘risida xabardor etishi shart.

O‘zbekiston Respublikasi jinoyat kodeksi:

143-modda. Xat-yozishmalar, telefonda so‘zlashuv, telegraf xabarlari yoki boshqa xabarlarning sir saqlanishi tartibini buzish

– Xat-yozishmalar, telefonda so‘zlashuv, telegraf xabarlari yoki boshqa xabarlarning sir saqlanishi tartibini qasddan buzish, shunday harakatlar uchun ma’muriy jazo qo‘llanilgandan keyin sodir etilgan bo‘lsa, eng kam oylik ish haqining yigirma besh baravarigacha miqdorda jarima yoki uch yilgacha muayyan huquqdan mahrum qilish yoki uch yuz oltmish soatgacha majburiy jamoat ishlari yoxud uch yilgacha axloq tuzatish ishlari bilan jazolanadi.

Kiberetika – kompyuterlar bilan bog‘liq falsafiy soha bo‘lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi, umuman insonlarga va jamiyatga qanday ta’sir ko‘rsatishini o‘rganadi. Kiberetika masalalariga quyidagi misollarni keltirish mumkin:

– Internetda boshqa odamlar to‘g‘risidagi shaxsiy ma’lumotlarni (masalan, onlayn holatlar yoki GPS orqali joriy joylashuvni) uzatish joizmi?

– foydalanuvchilarni soxta ma’lumotlardan himoya qilish kerakmi?

– raqamli ma’lumotlarga kim egalik qiladi (musiqa, filmlar, kitoblar, web-sahifalar va boshqalar) va ularga nisbatan foydalanuvchilar qanday huquqlarga ega?;

– onlayn qimor va pornografiya tarmoqda qanday darajada bo‘lishi kerak?

– Internetdan foydalanish har bir kishi uchun mumkin bo‘lishi kerakmi?

Mulk. Axborotdan foydalanishdagi etikaga oid munozaralar uzoq vaqtdan beri mulkchilik tushunchasini tashvishga solmoqda va kiberetika sohasidagi ko‘plab to‘qnashuvlarga sabab bo‘lmoqda. Egalikka oid nizolar egalik huquqi buzilgan yoki noaniq bo‘lgan hollarda yuzaga keladi.

Intellektual mulk huquqlari. Internet tarmog‘ining doimiy ravishda o‘sib borishi va turli ma’lumotlarni zichlash texnologiyalarining (masalan, mp3 fayl formati) paydo bo‘lishi “peer-ro-peer” fayl almashinuviga katta yo‘l ochdi. Bu imkoniyat dastlab Napster kabi dasturlar yordamida amalga oshirilgan bo‘lsa, endilikda BitTorrent kabi ma’lumotlarni uzatish protokollarida foydalanilmoqda. Uzatilgan musiqalarning aksariyati mualliflik huquqi bilan himoyalangan bo‘lsada, mazkur fayl almashinuvi noqonuniy hisoblanadi.

Hozirgi kunda aksariyat elektron ko‘rinishdagi media fayllar (musiqa, audio va kinofilmlar) intelektual mulk huquqlariga rioya qilinmasdan ommaga tarqalmoqda. Masalan, aksariyat katta mablag‘ sarflangan kinofilmlarning “qaroqchilarcha (piratskiy)” versiyasining chiqishi bois o‘z sarf xarajatlarini qoplay olmaslik holatlari kuzatilmoqda. Bu holatni dasturiy ta’minotlarda ham ko‘rish mumkin. Masalan, aksariyat dasturlar litsenziyaga ega hisoblansada, turli usullar yordamida ularning “darz ketgan (crack)” versiyalari amalda keng qo‘llaniladi. Masalan, litsenziyaga ega bo‘lmagan Windows 10 OT, antivirus dasturiy vositalari, ofis dasturiy vositalari va h.

Mualliflik huquqini himoyalashning texnik vositalari. Mualliflik huquqini ta’minlashda turli himoya usullaridan foydalaniladi. Ular CD/DVD disklardagi ma’lumotlarni ruxsatsiz ko‘chirishdan himoyalashdan tortib oddiy PDF fayllarni tahrirlash imkoniyatinicheklash kabi jarayonlarni o‘z ichiga olishi mumkin. Shu bilan birga, aksariyat insonlar litsenziyali CD diskni sotib olib, undan ko‘chirish imkoniyatiga ham ega bo‘lishim mumkin deb o‘ylaydilar.

Xavfsizlik. Internet tarmog‘idagi axborotdan xavfsiz foydalanish axloqiy munozaralar mavzusi bo‘lib kelmoqda. Bu birinchi navbatda jamoat faravonligini himoya qilish yoki shaxs huquqini himoya qilish masalasini o‘rtaga qo‘yadi. Internet tarmog‘idan foydalanuvchilar sonining ortishi, shaxsiy ma’lumotlarning ko‘payishi natijasida kiberjinoyatlar soni ortmoqda.

Ishonchlilik. Internetning mavjudligi va ba’zi bir shaxs yoki jamoalar tabiati tufayli ma’lumotlarning ishonchliligi bilan shug‘ullanish muammoga aylanmoqda. Boshqacha aytganda, Internetdagi ma’lumotlarning ishonchliligiga kim javob beradi? Bundan tashqari, Internetdagi ma’lumotlarni kim to‘ldirishi, undagi xatolar va kamchiliklar uchun kim javobgar bo‘lishi kerakligi to‘g‘risida ko‘plab tortishuvlar mavjud.

Foydalanuvchanlik, senzura va filtrlash. Foydalanuvchanlik, senzura va axborotni filtrlash mavzulari kiberetika bilan bog‘liq ko‘plab axloqiy masalalarni qamrab oladi. Ushbu masalalarning mavjudligi bizning maxfiylik va shaxsiylikni tushunishimizga va jamiyatdagi ishtirokimizga shubha tug‘diradi. Biror qonun qoidaga ko‘ra ma’lumotlardan foydalanishni cheklash yoki filtrlash asosida ushbu ma’lumotni tarqalishini oldini olish foydalanuvchanlikka ta’sir qilishi mumkin. Senzura ham past darajada (masalan, kompaniya o‘z xodimlari uchun) yoki yuqori darajada (hukumat tomonidan xavfsizlikni ta’minlash uchun amalga oshirilgan) bo‘lishi mumkin. Mamlakatga kiruvchi ma’lumotlarni boshqarishning eng yaxshi misollaridan biri - “Buyuk Xitoy Fayrvoli” loyihasi.

Axborot erkinligi. Axborot erkinligi, ya’ni, so‘z erkinligi, shu bilan birga ma’lumotni qidirish, olish va uzatish erkinligi kiberhujumda kimga va nimaga yordam beradi degan savol tug‘iladi. Axborot erkinligi huquqi, odatda, jamiyat yoki uning madaniyatiga ta’sir ko‘rsatadigan cheklovlarga bog‘liq. Cheklovlar turli ko‘rinishda bo‘lishi mumkin. Masalan, ayrim mamlakatlarda Internet ommaviy axborot vositalaridan foydalanishning bir shakli hisoblanib, undan barcha davlat rezidentlari foydalanadilar. Bundan tashqari, Internetdan foydalanish bo‘yicha cheklovlar ayrim davlatlarning turli shtatlarida farq qilishi mumkin.

Raqamli to‘siqlar. Axborot erkinligi bilan bog‘liq axloqiy masalalardan tashqari, *raqamli to‘siq* deb ataluvchi muammo turi mavjud bo‘lib, u kiberfazodan foydalanish imkoniyati cheklanganlar o‘rtasidagi ijtimoiy tafovutni anglatadi. Dunyo mamlakatlari yoki mintaqalari o‘rtasidagi bu tafovut global raqamli to‘siq deb ataladi.

Taqiqlangan kontentlar (pornografiya). Internet tarmog‘ida mavjud bo‘lgan taqiqlangan kontentlarni voyaga yetmaganlar tomonidan foydalanish doimo axloqiy munozaralarga sabab bo‘lgan. Ayrim davlatlarda bunday kontentlardan foydalanish qat’iy taqiqlansa, ayrim davlatlarda bunga ruxsat berilgan.

Kompyuter o‘yinlari. Bu muammo ham etik masaladagi munozaralardan biri, uni kimlardir zarar deb hisoblasa, yana kimlardir ularga qonunaralashuvini yoqtirmaydilar. O‘z navbatida tomonlar orasida “Qaysi turdagi o‘yinlarga ruxsat berish kerak? Ular qayerda o‘tkazilishi kerak?”degan savollar keng munozaralarga sabab bo‘lmoqda. Hozirda aksariyat davlatlarda bu turdagi o‘yinlarga qonuniy ruxsat berilgan bo‘lsa, qolganlarida qat’iy cheklovlar mavjud.

Kompyuterdan foydalanish etikasi. Kompyuterdan foydalanish etikasi instituti notijoriy tashkilot bo‘lib, vazifasi texnologiyani axloqiy nuqtai nazaridan targ‘ib qilish hisoblanadi. Ushbu tashkilot tomonidan quyidagi 10 ta etika qoidalari keltirib o‘tilgan:

– shaxsiy kompyuteringizdan boshqalarning zarariga foydalanmang;

– boshqa foydalanuvchilarning kompyuter ishlariga xalaqit bermang;

– boshqa foydalanuvchilarning kompyuter fayllariga qaramang;

– o‘g‘irlik maqsadida kompyuterdan foydalanmang;

– yomonlik maqsadida kompyuterdan foydalanmang;

– o‘z pulingizga sotib olmagan dasturdan foydalanmang va nusxa ko‘chirmang;

– birovning kompyuteridan ruxsatsiz foydalanmang;

– birovlarni intellektual mehnati samarasiga zarar yetkazmang;

– siz yaratgan dasturning ijtimoiy oqibati haqida o‘ylang;

– o‘z kompyuteringizdan boshqalarga nisbatan ongli va hurmat bilan foydalaning.

Axborotdan oqilona foydalinish kodeksi. Axborotdan oqilona foydalanish kodeksi buxgalteriya tizimiga qo‘yiladigan talablarni ta’kidlaydigan beshta prinsipga asoslanadi. Ushbu talablar AQSh sog‘liqni saqlash va insonlarga xizmat ko‘rsatish vazirligi tomonidan 1973 yilda kiritilgan:

– shaxsiy ma’lumotlarni to‘playdigan tizimlar bo‘lmasligi kerak;

– har bir kishi tizimda u to‘g‘risida qanday ma‘lumotlar saqlanishini va undan qanday foydalanilishini boshqarishi kerak;

– har bir kishi o‘zi to‘g‘risida to‘plangan ma’lumotlardan belgilangan maqsadda foydalanilishini nazoratlash imkoniyatiga ega bo‘lishi kerak;

– har kim o‘zi haqidagi ma’lumotlarni to‘g‘rilashi kerak;

– shaxsiy ma’lumotlar sirasiga kiruvchi ma’lumotlar to‘plamini yaratish, saqlash, ishlatish yoki tarqatish bilan shug‘ullanadigan har bir tashkilot ushbu ma’lumotlardan faqat belgilangan maqsadlar uchun foydalanilishni ta’minlash va boshqa maqsadlarda foydalanilishga qarshi choralar ko‘rishi kerak.

1.3. Inson faoliyati xavfsizligi

Ijtimoiy (sotsial) injineriya - turli psixologik usullar va firibgarlik amaliyotining to‘plami, uning maqsadi firibgarlik yo‘li bilan shaxs to‘g‘risida maxfiy ma’lumotlarni olish. Maxfiy ma’lumotlar - foydalanuvchi ismi/ parollari, shaxsiy ma’lumotlari, ayblov dalillari, bank karta raqamlari va moliyaviy yoki obro‘sini yo‘qotadigan har qanday ma’lumot.

Mazkur atama xakerlik sohasidan kirib kelgan, *xaker* - kompyuter tizimidagi zaifliklarni qidiradigan odam, boshqacha aytganda “buzg‘unchi”. Hozirgi vaqtda xakerlar har qanday tizimdagi asosiy zaiflik - mashina emas, balki shaxs ekanligini yaxshi tushunishadi. Inson, xuddi kompyuter singari, muayyan qonunlarga muvofiq ishlaydi. Psixologiya, hiyla-nayranglar va ta’sir mexanizmlari doirasida insoniyat tomonidan to‘plangan tajribadan foydalangan holda, xakerlar “odamlarga hujum qilishni” boshlaydilar. Gohida ularni “aql xakerlari” deb ham atashadi.

Masalan, xaker sizdan pul olmoqchi deb faraz qilaylik. Aytaylik, u sizning telefon raqamingiz va ijtimoiy tarmoqdagi akkauntingiz haqida ma’lumotga ega. Bundan tashqari, u izlanish natijasida sizning akangiz borligini ham aniqladi va akangiz haqida ham yetarlicha ma’lumot to‘pladi. U shuningdek, akangizning telefon raqamini ham biladi. Shundan so‘ng, ushbu ma’lumotlar asosida o‘z rejasini tuza boshladi.

Reja: Xaker sizga kechki vaqtda telefon qilib, sizga (sizni ismingiz o‘rniga faqat akangiz ataydigan biror “laqab” ham bo‘lishi mumkin) men akangman deb tanishtiradi va o‘zini ko‘chada bezorilarga duch kelganini, ular barcha narsalarini (telefon, pul, plastik kartochka va h.) olib qo‘yganini aytadi. Bundan tashqari, u o‘ziga bir qiz yordam berganini, biroq, uning yonida puli yo‘qligini aytadi. Shu bilan birga, ushbu qizni yonida plastik kartasi borligini va sizdan ushbu plastik kartaga kasalxonaga yetib borish uchun zarur bo‘lgan 20 000 so‘m pulni ko‘chirib berishni talab qiladi. Mazkur holatlarning 80% da xakerlar muvaffaqqiyatga erishganlar va bu ishlarni amalga oshirish malakalixaker uchun qiyinchilik tug‘dirmaydi.

Mazkur holda akangizni ovozini ajratish imkoniyati haqida gap borishi mumkin. Biroq, inson turli hayojon va shovqin bo‘lgan muhitda bo‘lishi mumkin. Bundan tashqari, agar siz uxlab yotgan vaqtingizda telefon bo‘lsa, ovozni aniqlashingiz yanada qiyinlashadi.

Ushbu holatda xaker tomonidan foydalanilgan fikrlarni ko‘rib chiqaylik:

1. Shaxsini yaxshi yashirgan va real misollarga asoslangan (masalan, sizning rasmlaringiz, faqat sizning yaqinlaringiz biladigan joylar va h.) va yaxshi afsona o‘ylab topdi.

2. Bularning barchasi yetarlicha tez va ishonchli tarzda aytilgan.

3. Ta’sirning juda ishonarli mexanizmidan foydalanilgan – achinishga majbur qilingan (hissiyotlarga murojaat qilish).

Sotsial injineriya bilan bog‘liq tahdidlarni quyidagicha tasniflash mumkin:

Telefon bilan bog‘liq tahdidlar. Telefon hanuzgacha tashkilotlar ichida va ular o‘rtasidagi aloqaning eng keng tarqalgan usullaridan biri hisoblanadi. Shuning uchun, u sotsial injineriya uchun samarali vosita bo‘lib qolmoqda. Telefonda gaplashayotganda, suhbatdoshining shaxsini tasdiqlashning imkoni yo‘q. Bu hujumchilarga xodimning, xo‘jayinning maxfiy yoki muhim tuyuladigan ma’lumotlarga ishonishi mumkin bo‘lgan har qanday shaxsning o‘rnida bo‘lish imkonini beradi. Bunda, zo‘ravonlik qurbonining “yordam berishdan” boshqa imkoni qolmaydi. Hattoki, uyushtiriladigan suhbat ahamiyatsiz bo‘lib ko‘ringan taqdirda ham.

Uyali telefondan foydalanuvchilarni pul o‘g‘irlashga qaratilgan firibgarlikning turli usullari mavjud. Bunga qo‘ng‘iroqlar yoki lotereyalardagi yutuqlar, SMS-xabarlar, xatoliklar orqali pulni qaytarish to‘g‘risidagi so‘rovlar yoki jabrlanuvchining yaqin qarindoshlari muammoga duch kelganligi hamda ma’lum miqdordagi pulni zudlik bilan o‘tkazish kerakligi haqidagi xabarlarni keltirish mumkin.

Mazkur hollarda quyidagi xavfsizlik choralarini amalga oshirish talab etiladi:

- telefon qiluvchining shaxsini aniqlash;
- raqamni aniqlash xizmatidan foydalanish;
- SMS – xabardagi noma’lum havolalarga e’tibor bermaslik.

Elektron pochta bilan bog‘liq tahdidlar. Ko‘pgina xodimlar har kuni korporativ va shaxsiy pochta tizimlaridan o‘nlab, hatto yuzlab elektron pochta xabarlarini qabul qilishadi. Albatta, bunday yozishmalar oqimining har bir harfiga yetarlicha e’tibor berishning imkoni yo‘q. Bu esa hujumlarni amalga oshirishni sezilarli darajada osonlashtiradi. Elektron pochta tizimlarining ko‘plab foydalanuvchilari bunday holni bir papkadan ikkinchisiga qog‘ozlarni o‘tkazishning elektron analogi sifatida qabul qilishadi va xabarlarni qabul qilishda xotirjam bo‘lishadi. Tajovuzkor pochta orqali oddiy so‘rov yuborganida, uning qurboni ko‘pincha uning xatti-harakatlari haqida o‘ylamasdan ular so‘ragan ishni

bajaradi. Elektron pochtalarda xodimlarni korporativ atrof-muhit muhofazasini buzishga undaydigan giperhavolalar bo‘lishi mumkin. Bunday havolalar har doim ham da’vo qilingan sahifalarga murojaat qilmaydi.

Xavfsizlik choralarining aksariyati ruxsatsiz foydalanuvchilarning korporativ resurslardan foydalanishini oldini olish uchun ishlab chiqilgan. Buzg‘unchi tomonidan yuborilgan giperhavolaga murojaat orqali foydalanuvchining zararli dasturni korporativ tarmoqqa yuklashi ko‘plab himoya turlarini chetlab o‘tishga imkon beradi. Giperhavola, shuningdek, ma’lumot yoki yordamni talab qiladigan qalqib chiquvchi ilovalar bilan turli xostlarga murojaatni talab qilishi mumkin. Firibgarlikni va zararli hujumlarni oldini olishning eng samarali usuli - kutilmagan foydalanuvchining elektron pochtasi xabarlariga shubha bilan qarash. Ushbu yondashuvni butun tashkilotda tarqatish uchun xavfsizlik siyosatida belgilangan elektron pochtadan foydalanishning quyidagi elementlari kiritilishi kerak:

- hujjatlarga qo‘shimchalar;
- hujjatdagi giperhavolalar;
- shaxsiy yoki korporativ ma’lumotlarni kompaniya ichida so‘rash;
- shaxsiy yoki korporativ ma’lumotlarga kompaniya tashqarisidan keladigan so‘rovlar.

Tezkor xabarlardan foydalanishga asoslangan tahdidlar. Tezkor xabar almashish - ma’lumotlarni uzatishning nisbatan yangi usuli. Ammo, u korporativ foydalanuvchilar orasida allaqachon mashhurlikka erishgan. Foydalanishning tezligi va qulayligi tufayli ushbu aloqa usuli turli xil hujumlar uchun keng imkoniyatlarni ochib beradi. Foydalanuvchilar unga telefon kabi qarashadi va uni bo‘lishi mumkin bo‘lgan dasturiy tahdidlar sifatida baholashmaydi. Tezkor xabarlar xizmatidan foydalanishga asoslangan hujumlarning ikkita asosiy turi - zararli dasturga havola va dasturning o‘zi haqida xabarning ko‘rsatilishi hisoblanadi. Tezkor xabarlar xizmatlarining xususiyatlaridan biri - aloqaning norasmiyligi, unda har qanday nomlarni moslashtirish qobiliyati bilan bir qatorda, bu omil tajovuzkorni o‘zini boshqa odam bo‘lib ko‘rsatishiga imkon beradi. Bu esa muvaffaqiyatli hujum qilish ehtimolini sezilarli darajada oshiradi. Agar kompaniya tezkor xabarlar sababli keladigan xarajatlarni kamaytirish maqsadida boshqa afzalliklardan foydalanmoqchi bo‘lsa, korporativ xavfsizlik siyosatida tegishli tahdidlardan himoya qilish mexanizmlarini ta’minlashi kerak. Korporativ muhitda tezkor xabar

almashish ustidan ishonchli boshqaruvga ega bo‘lish uchun quyidagi talablar bajarilishi shart:

- tezkor xabarlar uchun bitta platformani tanlash;
- tezkor xabar yuborish xizmatini o‘rnatishda xavfsizlik sozlamalarini aniqlash;
- yangi aloqalarni o‘rnatish prinsiplarini aniqlash;
- parol tanlash standartlarini o‘rnatish;
- tezkor xabarlardan foydalanish bo‘yicha tavsiyalar berish.

Sotsial injineriya mutaxassislari tashkilotlar uchun quyidagi asosiy himoya usullarini qo‘llashni tavsiya etishadi:

- muhim ma’lumotlar ko‘rinishida bo‘lgan, zararsiz ko‘rinadigan ma’lumot turlarini hisobga oladigan ishonchli ma’lumotlarni tasniflash siyosatini ishlab chiqish;
- ma’lumotlarni shifrlash yoki foydalanishni boshqarish yordamida mijoz ma’lumotlari xavfsizligini ta’minlash;
- xodimlarni sotsial injineriya ko‘nikmalariga o‘rgatish, ularni o‘zlari tanimaydigan odamlar bilan muloqotiga shubha bilan qarashni o‘rgatish;
- xodimlar orasida parollarni almashishni yoki umumiy foydalanishni taqiqlash;
- shaxsan tanish bo‘lmagan yoki biron-bir tarzda tasdiqlanmagan shaxsga korxonaga tegishli ma’lumotlarni berishni taqiqlash;
- maxfiy ma’lumotlardan foydalanishni so‘raganlar uchun maxsus tasdiqlash muolajalaridan foydalanish.

Sotsial injineriya hujumlarini oldini olishda ko‘p hollarda kompaniyalar tomonidan murakkab, ko‘p darajali xavfsizlik tizimlari qo‘llaniladi. Bunday tizimlarning ba’zi xususiyatlari va majburiyatlari quyida keltirilgan:

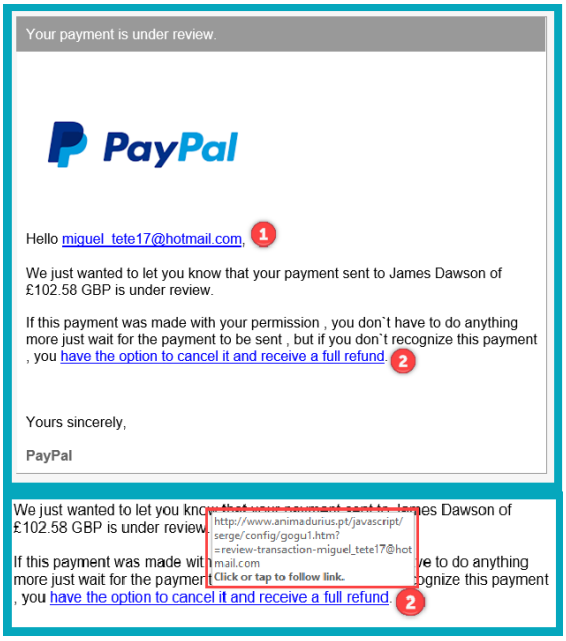
- *Fizik xavfsizlik.* Kompaniya binolari va korporativ resurslardan foydalanishni cheklaydigan to‘siqlar. Unutmaslik kerakki, kompaniyaning resurslari, masalan, kompaniya hududidan tashqarida joylashgan axlat konteynerlari fizik himoyalanmagan.
- *Ma’lumotlar.* Biznes ma’lumotlari: qayd yozuvlari, pochta va boshqalar bo‘lib, tahdidlarni tahlillash va ma’lumotlarni himoya qilish choralarini rejalashtirishda qog‘oz, elektron ma’lumot eltuvchilari bilan ishlash prinsiplarini aniqlash kerak.
- *Ilovalar* - foydalanuvchilar tomonidan boshqariladigan dasturlar. Atrofini himoya qilish uchun elektron pochta dasturlaridan,

tezkor xabarlar xizmati va boshqa dasturlardan tajovuzkorlar qanday foydalanishlari mumkinligini ko‘rib chiqish kerak.

- *Kompyuterlar*. Korporativ kompyuterlarda qaysi dasturlardan foydalanish mumkinligini ko‘rsatadigan qat’iy prinsiplarni belgilash, foydalanuvchilar kompyuterlariga to‘g‘ridan-to‘g‘ri hujumlardan himoya qilish.
- *Ichki tarmoq*. Korxona tizimlariga ta’sir qiladigan tarmoq, u mahalliy, global yoki simsiz bo‘lishi mumkin. So‘nggi yillarda masofadan ishlaydigan usullarning ommaviylashi sababli, ichki tarmoqlarning chegaralari sezilarli darajada o‘zboshimchalik bilan kengaytirildi. Kompaniya xodimlari har qanday tarmoq muhitida xavfsiz ishlarni tashkil qilishda nima qilish kerakligini tushunishlari lozim.
- *Tarmoq perimetri.* Kompaniyaning ichki tarmoqlari va tashqi, masalan, Internet yoki hamkor tashkilotlar tarmoqlari o‘rtasidagi chegara.

Sotsial injineriyaga tegishli ko‘plab hujumlar mavjud, quyida ularning ayrimlari keltirilgan:

Fishing. Fishing (ing. Phishing – baliq ovlash) Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan (login/parol) foydalanish imkoniyatiga ega bo‘lish. Bu hozirda keng tarqalgan sotsial injineriya sxemalaridan biri hisoblanadi. Katta hajmdagi shaxsiy ma’lumotlarni keng tarqalishi, fishing “shamolisiz” amalga oshmaydi. Fishingning eng keng tarqalgan namunasi sifatida jabrlanuvchining elektron pochtasiga yuborilgan rasmiy ma’lumot ko‘rinishidagi bank yoki to‘lov tizimining soxta xabarini ko‘rsatish mumkin. Bunday elektron pochta xabarlari odatda rasmiy web-saytga o‘xshash va shaxsiy ma’lumotlarni talab qiladigan shakldagi qalbaki web sahifaga havolani o‘z ichiga oladi (1.5-rasm). Rasmda keltirilgan birinchi holatda mijozning yoki foydalanuvchining ismi va familiyasini yozish o‘rniga pochta manzili yozilgan bo‘lsa, ikkinchi holatda ko‘rsatilgan havola ustiga sichqoncha olib borilganida, haqiqiy manzilni (www.PayPal.com) emas, balki, boshqa manzilni ko‘rish mumkin.



1.5-rasm. Fishing hujumiga misol

Quyida keng tarqalgan fishing sxemalariga misollar keltirilgan.

Mavjud bo‘lmagan havola. Fishing hujumining mazkur turida biror web saytga o‘xshash web saytga murojaat amalga oshirilishi tavsiya etiladi. Masalan, www.PayPai.com manzilini www.PayPal.com manzili sifatida yuborish mumkin. Bu holda kamdan-kam holda foydalanuvchilar “l” harfini o‘riniga “i” harfi borligiga e’tibor berishadi. Havolaga murojaat qilinganida esa www.PayPal.com web saytga o‘xshash, biroq soxta web saytga tashrif buyuriladi va talab kiritilgan to‘lov kartasi ma’lumotlari kiritiladi. Natijada, kiritilgan ma’lumotlar xaker qo‘liga tushadi.

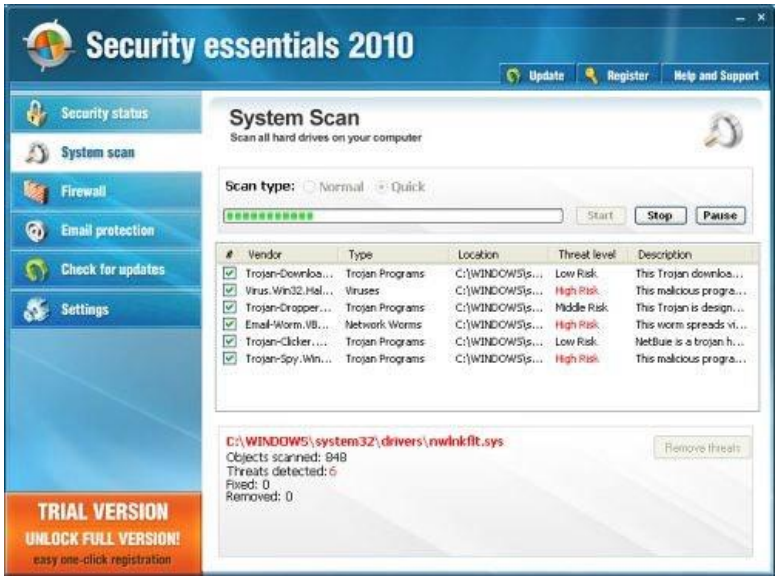
Bunga yaqqol misol sifatida, 2003 yilda eBay foydalanuvchilariga tarqalgan fishing xabarni keltirish mumkin. Mazkur xabarda foydalanuvchilarning akkauntlari blokirovkalangani va kredit karta ma’lumotlari blokirovkadan chiqarilishi kerakligi keltirilgan va unda rasmiy web-saytga o‘xshash soxta web saytga olib boruvchi havola mavjud bo‘lgan. Ushbu fishing hujumining keltirgan zarari bir necha yuz ming dollarga teng bo‘lgan.

Taniqli korporativ brendidan foydalanishga asoslangan firibgarlik. Firibgarlikning mazkur ko‘rinishida taniqli yoki yirik kompaniyalar nomidan foydalanuvchiga xabar yuboriladi. Xabarda kompaniya tomonidan o‘tkazilgan biror tanlovda g‘alaba qozonilganligi haqidagi tabriklar bo‘lishi mumkin. Unda shuningdek, zudlik bilan qayd yozuvi ma’lumotlari va parolni o‘zgartirish kerakligi so‘raladi. Shunga o‘xshash

sxemalar texnik ko‘maklashish xizmati nomidan ham amalga oshirilishi mumkin.

Soxta lotareyalar. Mazkur fishing sxemasiga ko‘ra foydalanuvchi har qanday taniqli kompaniya tomonidan o‘tkazilgan lotereyada g‘olib bo‘lgani to‘g‘risidagi xabarni olishi mumkin. Tashqi tomondan, bu elektron xabar kompaniyaning yuqori lavozimli xodimlaridan biri nomidan yuborilganga o‘xshaydi.

Soxta antivirus va xavfsizlik dasturlari. Mazkur dasturlar firibgar dasturiy ta‘minoti yoki “chaqqon dastur” deb nomlanib, ular antivirus dasturlariga o‘xshasada, vazifasi boshqacha. Bu dasturiy ta’minot turli tahdidlar to‘g‘risidagi yolg‘on xabarnomalar asosida foydalanuvchini soxta bitimlarga jalb qilishga harakat qiladi. Foydalanuvchi ulardan foydalanganida elektron pochtada, onlayn e’lonlarda, ijtimoiy tarmoqlarda, qidiruv tizimlari natijalarida va hatto foydalanuvchi kompyuterida turli qalqib chiquvchi oynalarga duch kelishi mumkin. Quyida keltirilgan misolda, aslida Microsoft Security Essentials bo‘lishi kerak bo‘lgan, biroq o‘ziga Security Essentials 2010 nomi berilgan soxta antivirus dasturining ko‘rinishi keltirilgan (1.6-rasm).



1.6-rasm. “Security Essentials 2010” antivirus dasturi

IVR (Interactive Voice Response) yoki telefon orqali fishing. Fishing sxemasining mazkur usuli oldindan yozib olingan xabarlar tizimidan foydalanishga asoslangan, ular bank va boshqa IVR tizimlarining “rasmiy qo‘ng‘iroqlari”ni qayta tiklash uchun ishlatiladi. Bu hujumda jabrlanuvchi bank bilan bog‘lanib, qandaydir ma’lumotlarni tasdiqlash yoki yangilash kerakligi haqidagi so‘ovni qabul qiladi. Tizim PIN kodni

yoki parolni kiritish orqali foydalanuvchi tasdig‘ini talab qiladi. Natijada, muhim ma’lumotlarni qo‘lgan kiritgan buzg‘unchi foydalanuvchi ma’lumotlaridan foydalanish imkoniyatiga ega bo‘ladi. Masalan, parolni almashtirish uchun “1” ni bosing va operator javobini olish uchun “2” ni bosing va h.

Pretekstinq. Mazkur fishing sxemasida xaker o‘zini boshqa shaxs sifatida ko‘rsatadi va oldindan tayyorlangan senariy (skript) bo‘yicha maxfiy axborotni olishni maqsad qiladi. Ushbu hujumda qurbonni shubhalanmasligi uchun tegishli tayyorgarlik ko‘riladi: tug‘ilgan kun, INN, pasport raqami yoki hisob raqamining oxirgi belgilari kabi ma’lumotlar topiladi. Ushbu fishing sxemasi odatda telefon yoki elektron pochta orqali amalga oshiriladi.

Kvid pro kvo (lotinchadan: Quid pro quo). Ushbu ibora ingliz tilida “*xizmat uchun xizmat*” degan ma’noni anglatib, sotsial injineriyaning mazkur turida xaker korporativ tarmoq yoki elektron pochta orqali kompaniyaga murojaatni amalga oshiradi. Ko‘pincha xaker o‘zini texnik xizmat ko‘rsatuvchi sifatida tanitib, texnik xodimning ish joyidagi muammolarni bartaraf etishda “yordam berishini” aytadi. Texnik muammoni “bartaraf” etish vaqtida nishondagi shaxsni buyruqlarni bajarishga yoki jabrlanuvchining kompyuteriga turli xil dasturlarni o‘rnatishga undash amalga oshiriladi. Masalan, 2003 yilda Axborot xavfsizligi dasturi doirasida o‘tkazilgan tadqiqot ofis xodimlarining 90% har qanday xizmat yoki to‘lov uchun maxfiy ma’lumotlarni, masalan, o‘zlarining parollarini, berishga tayyor bo‘lishini ko‘rsatdi.

Yo‘l-yo‘lakay olma. Sotsial injineriyaning mazkur usulida xaker maxsus zararli dastur yozilgan ma’lumot eltuvchilardan foydalanadi va zararli dasturlar yozilgan eltuvchilarni qurbonning ish joyi yaqinida, jamoat joylarida va boshqa joylarda qoldiradi. Bunda, ma’lumot eltuvchilari tashkilotga tegishli shaklda rasmiylashtiriladi. Masalan, xaker biror korporatsiya logotipi va rasmiy web-sayt manzili tushirilgan kompakt diskni qoldirib ketadi. Ushbu disk “Rahbarlar uchun ish haqlari” nomi bilan nomlanishi mumkin. Ushbu eltuvchini qo‘lga kiritgan qurbon uni o‘z kompyuteriga qo‘yib ko‘radi va shu orqali kompyuterini zararlaydi.

Ochiq ma’lumot to‘plash. Sotsial injineriya texnikasi nafaqat psixologik bilimlarni, balki, inson haqida kerakli ma’lumotlarni to‘plash qobilyatini ham talab etadi. Bunday ma’lumotlarni olishning nisbatan yangi usuli ochiq manbalardan, ijtimoiy tarmoqlardan to‘plash. Masalan, «Одноклассники», «ВКонтакте», «Facebook», «Instagram» kabi

saytlarda odamlar yashirishga harakat qilmaydigan juda ko‘p ma’lumotlar mavjud. Odatda, foydalanuvchilar xavfsizlik muammolariga yetarlicha e’tibor bermasdan, xaker tomonidan foydalanilishi mumkin bo‘lgan ma’lumotlar va xabarlarni qarovsiz qoldiradilar.

Bunga yaqqol misol sifatida Yevgeniy Kasperskiyning o‘g‘lini o‘g‘irlanganini keltirish mumkin. Mazkur holatda jinoyatchilar o‘smirning kun tartibini va marshrutini ijtimoiy tarmoq sahifalaridagi yozuvlardan bilgani aniqlangan.

Ijtimoiy tarmoqdagi o‘z sahifasidagi ma’lumotlardan foydalanishni cheklab qo‘ygan taqdirda ham, foydalanuvchining firibgarlik qurboni bo‘lmasligiga to‘liq kafolat yo‘q. Masalan, Braziliyaning kompyuter xavfsizligi bo‘yicha tadiqiqotchisi 24 soat ichida sotsial injineriya usullaridan foydalangan holda har qanday Facebook foydalanuvchisibilan do‘stlashish mumkinligini ko‘rsatdi. Tajriba davomida Nelson Novayes Neto dastlab jabrlanuvchiga tanish bo‘lgan odam – uning xo‘jayini uchun soxta qayd yozuvini yaratadi. Avval Neto jabrlanuvchining xo‘jayinining do‘stlariga va undan keyin to‘g‘ridan- to‘g‘ri jabrlanuvchining do‘stiga do‘stlik so‘rovini yuboradi. 7,5 soatdanso‘ng esa tadqiqotchi jarblanuvchi bilan do‘stlashadi. Natijada tadqiqotchi foydalanuvchining shaxsiy ma’lumotlarini olish ikoniyatiga ega bo‘ladi.

Yelka orqali qarash. Ushbu hujumga ko‘ra buzg‘unchi jabrlanuvchiga tegishli ma’lumotlarini uning yelkasi orqali qarab qo‘lga kiritadi. Ushbu turdagi hujum jamoat joylarida, masalan, kafe, avtobus, savdo markazlari, aeroport va temir yo‘l stansiyalarida keng tarqalgan. Mazkur hujumga doir olib borilgan so‘rovnomalar quyidagilarni ko‘rsatgan:

- 85% ishtirokchilar o‘zlari bilishlari kerak bo‘lmagan maxfiy ma’lumotlarni ko‘rganliklarini tan olishgan;
- 82% ishtirokchilar ularning ekranidagi ma’lumotlarini ruxsatsiz shaxslar ko‘rishi mumkinligini tan olishgan;
- 82% ishtirokchilar tashkilotdagi xodimlar o‘z ekranini ruxsatsiz odamlardan himoya qilishiga ishonishmagan.

Teskari sotsial injineriya. Jabrlanuvchining o‘zi tajovuzkorga ma’lumotlarini taqdim qilishi teskari sotsial injineriyaga tegishli holat hisoblanadi. Bu bir qarashda ma’noga ega bo‘lmagan qarash hisoblansada, aksariyat hollarda jarblanuvchining o‘zi muammolarini hal qilish uchun tajovuzkorni yordamga jalb qiladi. Masalan, jabrlanuvchi bilan birga ishlovchi tajovuzkor jabrlanuvchi kompyuteridagi biror faylni

nomini o‘zgartiradi yoki boshqa katalogga ko‘chirib o‘tkazadi. Faylni yo‘‘q bo‘lganini bilgan qurbon esa ushbu muammoni tezda bartarafetishni istab qoladi. Bu vaziyatda tajovuzkor o‘zini ushbu muammoni bartaraf etuvchi sifatida ko‘rsatadi va qurbonning muammosini bartaraf etish bilan birga unga tegishli login/ parolni ham qo‘lga kiritadi. Bundantashqari, ushbu vazifasi bilan tajovuzkor tashkilot ichida obro‘ga ega bo‘ladi va o‘z qurbonlari sonini ortishiga erishadi. Bu holatni aniqlash esa ancha murakkab ish hisoblanadi.

Mashhur sotsial injinerlar. Kevin Mitnik tarixdagi eng mashhur sotsial injinerlardan biri, u dunyodagi mashhur kompyuter xakeri, xavfsizlik bo‘yicha mutaxassis va sotsial injineriyaga asoslangan kompyuter xavfsizligiga bag‘ishlangan ko‘plab kitoblarning ham muallifidir. Uning fikriga ko‘ra xavfsizlik tizimini buzishdan ko‘ra, aldash yo‘li orqali parolni olish osonroq.

Aka-uka Badirlar. Ko‘r bo‘lishlariga qaramasdan aka-uka Mushid va Shadi Badirlar 1990 yillarda Isroilda sotsial injineriya va ovozni soxtalashtirish usullaridan foydalangan holda bir nechta yirik firibgarlik sxemalarini amalga oshirishgan. Televideniyaga bergan intervyusida: “faqat telefon, elektr va noutbuklardan foydalanmaydiganlar uchun tarmoq xavfsizdir” deb aytishgan.

Sotsial injineriyadan himoyalanish choralari. Hujumlarni amalga oshirishda sotsial injineriya texnikasidan foydalangan tajovuzkorlar tez-tez muloyimlik, dangasalik, xushmuomilalik bilan foydalanuvchi va tashkilot xodimlarining qiziqishlaridan foydalanadilar. Hujumlarni oldini olish esa, xodimlarning aldanayotganliklarini bilmasliklari sababli, murakkab hisoblanadi.

Sotsial injineriya hujumlarini quyidagicha aniqlash mumkin:

- o‘zini do‘stingiz yoki yordam so‘rab murojaat qilgan yangi xodim sifatida tanishtirish;
- o‘zini yetkazib beruvchi, hamkor kompaniyaning xodimi yoki qonun vakili sifatida tanishtirish;
- o‘zini biror rahbar sifatida tanishtirish;
- biror zaiflikni bartaraf etuvchi yoki jabrlanuvchiga biror nimani yangilash imkoniyatini taqdim qiluvchi sotuvchi yoki ishlab chiqaruvchi sifatida tanishtirish;
- muammo yuzaga kelganida yordam beruvchi sifatida tanishtirish;
- ishonchni hosil qilish uchun ichki xotirjamlik va terminologiyadan foydalanish;

- “maktub”ga turli zararli dasturlarni qo‘shib yuborish;
- soxta ochilgan oynada login/ parolni qayta kiritishni so‘rash;
- foydalanuvchi nomi va paroli bilan saytga ro‘yxatdan o‘tish uchun biror sovg‘a taklif etish;
- jabrlanuvchi kompyuteriga yoki dasturiga kiritilgan kalitlarni yozib olish (keylogger dasturlari);
- turli xil zararli dasturiy vositaga ega ma’lumot eltuvchilarini foydalanuvchi stoliga tashlash;
- turli qo‘ng‘iroqlardagi ovozli xabarlar va h.

Hayotda ko‘plab jabhalarda sotsial injineriyaga tegishli muammolarni ko‘rish mumkin. Xususan, ommaviy madaniyatda (masalan, kinofilmlarda) sotsial injinerlikdan foydalanish holatlari tez-tez uchrab turadi. Masalan, quyidagi keltirilgan kinofilmlarda sotsial injineriyaga oid epizodlar mavjud:

- «Поймай меня, если сможешь»;
- «Поймай толстуху, если сможешь»;
- «Один дома»;
- «Хакеры»;
- «Афера Томаса Крауна»;
- «Бриллианты навсегда»;
- «Кто я».

Nazorat savollari

1. Axborot xavfsizligining hayotiy timsollari va ularning vazifalari.
2. Kiberxavfsizlik tushunchasiga izoh bering.
3. Kiberxavfsizlik fan sifatida qanday tuzilishga ega?
4. Kiberxavfsizlikning asosiy tushunchalari.
5. Axborotning konfidensialligini ta’minlash deganda nimani tushunasiz?
6. Axborotni yaxlitligini ta’minlash deganda nimani tushunasiz?
7. Axborot uchun foydalanuvchanlikning muhimligi.
8. Risk va uning kiberxavfsizlikdagi o‘rni.
9. Hujumchi kabi fikrlash nima uchun zarur?
10. Tizimli fikrlash nima va u nima uchun zarur?
11. Axborot xavfsizligi va axborotni himoyalash tushunchalarining bir-biridan farqi nimada?
12. Aktiv nima?

13. Tahdid va zaiflik tushunchalariga izoh bering.

14. Axborot xavfsizligi va kiberxavfsizlik tushunchalarining bir-biridan farqi nimada?

15. Kiberxavfsizlikning bilim sohalari va ularning asosiy xususiyatlari nimalardan iborat?

16. Kiberxavfsizlikda inson omilini misollar yordamida tushuntiring.

17. Kiberjinoyatchilik tushunchasiga izoh bering.

18. Kiberjinoyatni amalga oshirishdan ko‘zlangan maqsadlar.

19. Kiberjinoyatchilikning asosiy turlari.

20. Kiberetika tushunchasiga izoh bering va ularga misollar keltiring.

21. Kompterdan foydalanish davomida qanday etika qoidalarga e’tibor berish talab qilinadi?

22. Kiberjinoyatchilikni oldini olish usullari va kiberqonunlar haqida ma’lumot bering.

23. “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonunda axborotdan foydalanish tartiblari haqida nimalar deyilgan?

24. O‘zbekiston Respublikasining Ma’muriy javobgarlik to‘g‘risidagi kodeksida kiberjinoyatchilikka oid qanday bandlar mavjud?

25. O‘zbekiston Respublikasi jinoyat kodeksida kiberjinoyatchilikka oid qanday bandlar mavjud?

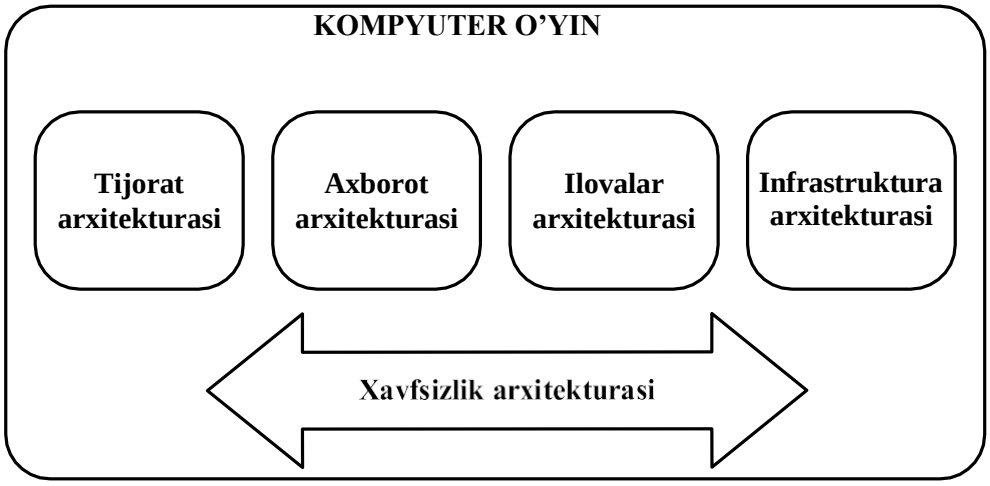
2 BOB. KIBERXAVFSIZLIK ARXITEKTURASI, STRATEGIYASI VA SIYOSATI

2.1. Kiberxavfsizlik arxitekturasi va strategiyasi

Zamonaviy tijorat oldida murakkab masalalar to‘plami ko‘ndalangki, beqaror iqtisodiy vaziyatda ularning dolzarbligi yanada oshadi. Bunday masalalarga quyidagilarni kiritish mumkin:

- daromadning oshishi;
- o‘zgaruvchi vaziyatlarga reaksiya tezligining oshishi;
- harajat va chiqimlarning pasayishi;
- innovatsiyaning tezlashishi;
- bozorga mahsulot va xizmatlarni taqdim etish vaqtining qisqarishi;
- buyurtmachilar va sheriklar xolisligining oshishi;
- raqobatlik qobiliyatining oshishi;
- me’yoriy talablarga moslikni ta’minlash.

Yuqorida keltirilgan barcha masalalarni yechishda korxona arxitekturasidan foydalaniladi (2.1-rasm). Korxona arxitekturasi prinsiplar, yondashishlar va texnologiyalar naborini shakllantirishga imkon beradiki, ular o’yinchining joriy holatini hisobga olgan holda uning kelgusi transformasiyasi, o‘sishi va rivojlanishi asosini belgilaydi.



2.1-rasm. Kompyuter o’yin yutug’lari va uning boshqa jamoalar bilan bog‘liqligi

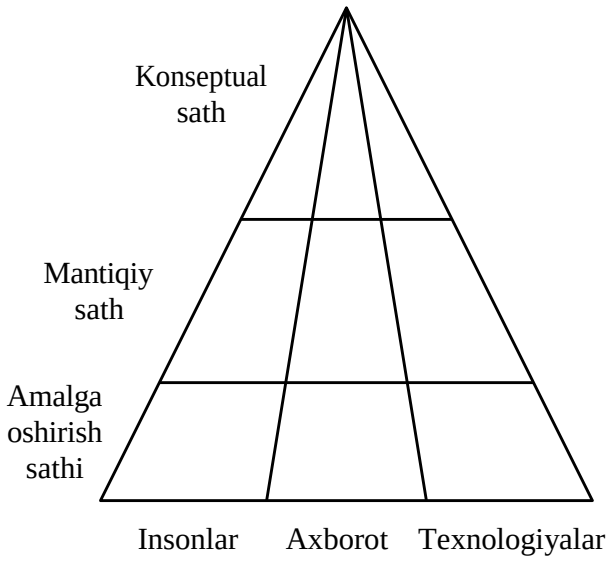
Hozirda bunday arxitekturalarni yaratishda bir necha yondashishlar mavjud, masalan TOGAF, Zachman Framework, FEAF, DoDAF va h.

Ammo, qaysi bir yondashish tanlanmasin, hozirgi sharoitda axborotdan va axborot tizimidan foydalanmay rivojlanish mumkin emas.

Axborot va axborot tizimlari nafaqat tijoratdagi har qanday o‘zgarishlarni madadlaydi, balki ularni oldindan sezadi, ularga oldindan tayyorlanadi, ba’zi xollarda esa yangi tijorat-imkoniyatlarining paydo bo‘lishiga yordam beradi. Biroq tijorat doimo istalgancha rivojlanmaydi. Bunda ma’lumotlarning sirqib chiqishi, axborot texnologiyalari infrastrukturasi elementlarining ishdan chiqishi va h. bilan bog‘liq axborot operatsion risklar anchagina rol o‘ynaydi. Hozirgi va kelajak risklarga tayyor bo‘lish uchun korxonaning boshqa arxitekturalari bilan uzviy bog‘langan axborot xavfsizligi arxitekturasi zarur.

Kiberxavfsizlik arxitekturasi jarayonlarni, inson rolini, texnologiyalarni va turli xil axborotni tavsiflaydi, hamda zamonaviy oyinlarning murakkabligini va o‘zgaruvchanligini hisobga oladi. Boshqacha aytganda, kiberxavfsizlikning arxitekturasi o’yinchining va u bilan bog‘liq boshqa komponentlar va interfeyslarning istalgan axborot xavfsizligi tizimi xolatini tavsiflaydi. Bunda axborot xavfsiziligi arxitekturasi tijoratning joriy va eng muhimi, kelgusidagi ehtiyojini akslantiradi.

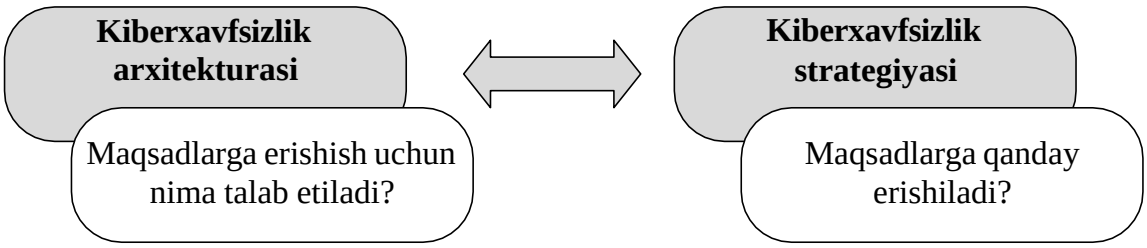
Odatda arxitekturaning 3 ta sathi ajratiladi – konseptual, mantiqiy va amalga oshirish (texnologik). 2.2-rasmda bunday arxitektura keltirilgan bo‘lib, odatda texnologiyalar jihatidagi qismi xavfsizlik xizmati nazoratidan chetda qoladi.



2.2-rasm. Kiberxavfsizlik arxitekturasi

Joriy holatdan qanday qilib yangi, mukammalroq va quyilgan maqsadlarga mos holatga o‘tish mumkin? Buning uchun strategiya, ya’ni quyilgan maqsadlarga erishish uchun harakat yo‘nalishi mavjud.

Strategiya – korxonaning davomli muvaffaqiyat bilan faoliyat yuritishini ta’minlashga mo‘ljallangan strukturalangan va o‘zaro bog‘langan harakatlar to‘plami. 2.3-rasmda arxitektura bilan strategiyaning o‘zaro bog‘liqligi keltirilgan. Strategiya kiberxavfsizlik arxitekturasi ko‘rinishidagi maqsadga ega bo‘lgan holda ungaerishishning optimal yo‘lini belgilaydi.



2.3-rasm. Arxitektura bilan strategiyaning o‘zaro bog‘liqligi

Ko‘pincha strategiya va arxitektura tushunchalarini farqlamay arxitektura tavsifini o‘z ichiga olgan kiberxavfsizlik strategiyasi ishlab chiqiladi. Bu unchalik to‘g‘ri emas, chunki arxitektura, ya’ni maqsadlar vaqt o‘tishi bilan o‘zgarmasligi, bu maqsadlarga erishishdagi strategiya esa tashqi va ichki omillarga bog‘liq holda jiddiy o‘zgarishi mumkin. Strategiya va arxitektura bitta hujjatda tavsiflansa, strategiya o‘zgarganida arxitekturani ham o‘zgartirishga to‘g‘ri keladi.

2.2. Kiberxavfsizlik siyosati va uni amalga oshirish

Axborot xavfsizligi siyosati (yoki xavfsizlik siyosati) – o’yinchining maqsadlari va vazifalari hamda xavfsizlikni ta’minlash sohasidagi tadbirlar tavsiflanadigan yuqori darajadagi reja. Siyosat xavfsizlikni umumlashgan atamalarda tavsiflaydi. U xavfsizlikni ta’minlashning barcha dasturlarini rejalashtiradi. Axborot xavfsizligi siyosati tashkilot masalalarini yechish jarayoni himoyasini yoki ish jarayoni himoyasini ta’minlashi shart.

Apparat vositalar va dasturiy ta’minot ish jarayonini ta’minlovchi vositalar hisoblanadi va ular xavfsizlik siyosati tomonidan qamrab olinishi shart. Shu sababli, asosiy vazifa sifatida tizimni (jumladan tarmoq xaritasini) to‘liq inventarizatsiyalashni ko‘zda tutish lozim. Tarmoq xaritasini tuzishda har bir tizimdagi axborot oqimini aniqlash lozim. Axborot oqimlari sxemasi axborot oqimlarining biznes-jarayonlarni qanchalik ta’minlayotganini, hamda axborotni himoyalash va yashovchanligini ta’minlash uchun qo‘shimcha choralarni ko‘rish muhim bo‘lgan soxani ko‘rsatishi mumkin. Undan tashqari, bu sxema yordamida

axborot ishlanadigan joyni, ushbu axborot qanday saqlanishi, qaydlanishi, joyini o‘zgartirishi va nazoratlanishi lozimligini aniqlash mumkin.

Inventarizatsiya apparat va dasturiy vositalardan tashqari dasturiy va apparatura hujjatlari, texnologik hujjat va h. kabi kompyuterga taalluqli bo‘lmagan resurslarni ham qamrab olishi shart. Ushbu hujjatlar tarkibida tijoratni tashkil etish xususiyatlari to‘g‘risidagi axborot bo‘lishimumkin va bu hujjatlar buzg‘unchilar foydalanishi mumkin bo‘lgan joylarni ko‘rsatadi.

Xavfsizlik siyosatining zaruriyati:

- Tashkilot bo‘ylab foydalanilayotgan qurilmalar soni ortib borishi tarmoqda uzatilayotgan va saqlanadigan axborot hajmini ortishiga olib kelmoqda. Bu holat esa o‘z navbatida turli zaifliklar natijasida hosil bo‘lgan xavfsizlik tahdidlarini ortishiga ham sababchi bo‘ladi. Xavfsizlik siyosati tashkilotga ushbu tahdidlarga qarshi kurashish va unga axborotning yo‘qolishidan himoyalash imkonini beradi.
- Xavfsizlik siyosati o’yinchining barcha funksiyalarini xavfsiz tarzda amalga oshirish orqali xavfsizlik prinsiplarining kelishilgan vazifalarini ta’minlaydi. Xavfsizlik siyosati mijozlar bilan ishonchga asoslangan aloqani qurishda axborot xavfsizligi standartlarining mosligini ta’minlaydi. Xavfsizlik siyosati tashqi axborot tahdidlariga kompaniyaning duchor bo‘lishi xavfini pasaytirishga yordam beradi.
- Xavfsizlik siyosati tarmoqda qanday qoidalar foydalanishi kerakligini, konfidensial axborot qanday saqlanishi va tashkilot ma’lumotlarini oshkor bo‘lishi va majburiyatlarni kamaytirish uchun qanday shifrlash algoritmlari kerakligini aniqlash orqali qonuniy himoyani ta’minlaydi.
- Xavfsizlik siyosati tahdidlarning sodir bo‘lishidan oldin ularni bashoratlash va zaifliklarni aniqlash orqali xavfsizlik buzilishlari holatining ehtimolini kamaytiradi.
- U shuningdek, zaxira nusxalash va qayta tiklash amallarini joriy qilish orqali tashkilot ma’lumotlarining yo‘qolishi va sirqib chiqishi xavfini minimallashtiradi.

Xavfsizlik siyosatining afzalliklari:

- *Kuchaytirilgan ma’lumot va tarmoq xavfsizligi:* tashkilotlar o‘z ma’lumotlari xavfsizligini ta’minlovchi tarmoqqa asoslangan siyosatini amalga oshiradilar. Xavfsizlik siyosati tarmoqda boshqa tizimlardan ma’lumotlar uzatilishida himoyani ta’minlaydi.
- *Risklarni kamaytirish:* xavfsizlik siyosatini amalga oshirish orqali tashqi manbalardan bo‘lishi mumkin bo‘lgan risklar kamaytiriladi.

Agar xodimlar xavfsizlik siyosati asosida harakat qilsalar, ma’lumot va resurslarning yo‘qolishi holatlari deyarli kuzatilmaydi.

- *Qurilmalardan foydalanish va ma’lumotlar transferining monitoringlanishi va nazoratlanishi:* xavfsizlik siyosati xodimlar tomonidan amalga oshirilgani bois, ma’murlar tashkilotdagi trafikni va foydalanilgan tashqi qurilmalarni doimiy tarzda monitoringlashi zarur. Kiruvchi va chiquvchi trafikning monitoringi va auditi doimiy ravishda amalga oshirilishi shart.
- *Tarmoqning yuqori unumdorligi:* xavfsizlik siyosati to‘g‘ri amalga oshirilganida va tarmoq doimiy monitoring qilinganida ortiqcha yuklamalar mavjud bo‘lmaydi. Tarmoqda ma’lumotni uzatish tezligi ortadi va bu umumiy samaradorlikni ortishiga olib keladi.
- *Muammolarga darhol javob berish va harakatsiz vaqtning kamligi:* xavfsizlik siyosatini amalga oshirilishi tarmoq muammolari kuzatilganida darhol javob berish imkoniyatini taqdim etadi.
- *Boshqaruvdagi hayajon darajasining kamayishi:* xavfsizlik siyosati amalga oshirilganida boshqaruvchi kam hayajonga ega bo‘ladi. Xavfsizlik siyosatidagi bir vazifa o’yinchining biror xodimiga biriktirilishi shart. Agar ushbu holat amalga oshirilsa, tarmoqda biror nojo‘ya holat kuzatilsa ham, boshqaruvda hech qanday xavotir bo‘lmaydi.
- *Xarajatlarning kamayishi:* agar xodimlar siyosatga to‘g‘ri amal qilsalar, tashkilotga ta’sir qiluvchi turli xalaqitlar uchun ortiqcha harajat kamayadi.

Xavfsizlik siyosatining iyerarxiyasi:

Tashkilotlarda xavfsizlik siyosatini ishlab chiqishda turli hujjatlardan foydalaniladi. Ushbu hujjatlarni ishlab chiqish xavfsizlik siyosatining iyerarxiyasining sathi va uning soniga bog‘liq.

- *Qonunlar.* Qonunlar iyerarxiyaning eng yuqori sathida joylashgan bo‘lib, ular tashkilotdagi har bir xodim amalga oshirishi kerak bo‘lgan vazifalarni o‘z ichiga oladi. Ushbu qonunlarga amal qilmagan har bir xodim uchun javobgarlik choralari ko‘rilishi shart bo‘ladi.
- *Normativ hujjatlar.* Normativ hujjatlar iyerarxiyadagi ikkinchi tashkil etuvchi bo‘lib, ular xodimlarning qonunlarga rioya qilishini kafolatlaydi. Normativ hujjatlar xavfsizlik siyosati qonuniga mos bo‘lgan yo‘l yo‘riq ko‘rsatuvchi hujjatlar to‘plami bo‘lib, ular hukumat yoki ijtimoiy normativ hujjatlardan tashkil topadi.
- *Siyosatlar.* Siyosatlar yordamida tashkilot shaxsiy tarmoq xavfsizligi uchun qonuniy ichki tarmoq talablarini yaratadi. Siyosat turli muolajalardan iborat bo‘lib, ular tashkilot uchun xavfsizlik arxitekturasini

ko‘rsatadi. Ushbu siyosatlarning amalga oshirilishi tashkilotga standartlarni o‘rnatish va risklarni boshqarish kabi vazifalarni bajarishiga imkon yaratadi.

- *Standartlar*. Standartlar siyosatni amalga oshirish usullarini tavsiflaydi va tashkilotlar tomonidan amalga oshiriladi. Standartlar korxona siyosatiga ixtiyoriy va mandatli aloqador bo‘lib, ishlab chiqilgan standartni ma’lum vaqtdan so‘ng o‘zgartirish talab etilmasligi zarur. Shuningdek, standartlar texnologiya, qurilma va dasturiy vositaga bog‘liq holda xavfsizlik nazoratini o‘z ichiga oladi.
- *Yo‘riqnomalar.* Yo‘riqnomalar tashkilot siyosati va standartlarini amalga oshirish strategiyasini aniqlab, o’yinchining tahdidlarga qarshi tura olishida yordam beradi. Shuning uchun, tashkilot xodimlari yo‘riqnomalarni bajarish uchun, maxsus o‘qitiladi.
- *Muolajalar*. Muoalajalar tashkilot siyosatini amalgaoshiruvchi ketma-ket bosqichlar to‘plami bo‘lib, ularni amalga oshirishdaimtiyozga ega subyektdan tasdiq talab etiladi. Muolajalar quyidagi savollar asosida ishlaydi:
  - kim nimani bajaradi?;
  - ular qanday bosqichlarga ega?;
  - ular qaysi shakl va hujjatlardan foydalanadilar?
- *Umumiy qoidalar*. Umumiy qoidalar tanlovga ko‘ra maslahatlar bilan ta’minlovchi hujjat bo‘lib, ulardan biror maxsus standartlar bo‘lmagan holda foydalaniladi. Umumiy qoidalar tavsiyalar sifatida bo‘ladi va tashkilotlar ularni rad eta olmaydi. Umumiy qoidalarni amalga oshirish risklarni kamaytirsada, biznes talablari o‘zgarganida umumiy qoidalarni ham o‘zgartirish tavsiya etiladi.

Xavfsizlik siyosati quyidagi xususiyatlarga ega bo‘lishi shart:

- *Qisqa va aniq:* xavfsizlik siyosati infrastrukturada joriy qilishda qisqa va aniq bo‘lishi shart. Murakkab xavfsizlik siyosati tushunish uchun qiyin bo‘lib, xodimlar tomonidan kutilgani kabi amalga oshirilmaydi.
- *Foydalanuvchan bo‘lishi:* siyosat o’yinchining turli sektorlari bo‘ylab oson foydalanishli yozilishi va loyihalanishi shart. Yaxshi yozilgan siyosatlar boshqarishga va amalga oshirishga oson bo‘ladi.
- *Iqtisodiy asoslangan bo‘lishi:* tashkilotlar tejamkor va o‘z xavfsizligini kuchaytiruvchi siyosatni amalga oshirishlari shart.
- *Amaliy bo‘lishi:* siyosatlar reallikka asoslangan amaliy bo‘lishi kerak. Real bo‘lmagan siyosatning amalga oshirilishi tashkilotga muammo tug‘diradi.

- *Barqaror bo‘lishi:* tashkilot o‘zining siyosatini amalga oshirishda barqarorlikga ega bo‘lishi kerak.
- *Mulojaviy bardoshli bo‘lishi:* siyosat muolajalari amalga oshirilganida, ular ish beruvchi va ishlovchiga mos bo‘lishi kerak.
- *Kiber va yuridik qonunlarga, standartlarga, qoidalarga va yo‘riqnomalarga mos bo‘lishi:* amalga oshiriluvchi ixtiyoriy siyosat kiber qonunlar asosida ishlab chiqilgan qoidalar va yo‘riqnomalarga mos bo‘lishi zarur.

Axborot xavfsizligi siyosatining turlari. Tashkilotda axborot xavfsizligini rejalashtirish, loyihalash va amalga oshirishda siyosat muhim hisoblanib, ular foydalanuvchilarga xavfsizlik maqsadlariga erishishda mavjud muammolarni bartaraf etish choralarini taqdim etadi. Bundan tashqari, xavfsizlik siyosati tashkilotdagi dasturiy ta’minot va jihozlar vazifasini tavsiflaydi.

Axborot texnologiyalari sohasidagi korxonalarda quyidagi xavfsizlik siyosatlari qo‘llaniladi:

- *Tashkilot axborot xavfsizligi siyosati (Enterprise Information Security Policies, EISP):* mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi. Bundan tashqari, ushbu siyosat taklif etilgan va talab qilingan axborot xavfsizligi strukturasi talablarini kafolatlaydi.
- *Muammoga qaratilgan xavfsizlik siyosatlari (Issue-Specific Security Policies, ISSP):* bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi. Unda profilaktik choralar, masalan, foydalanuvchilarning foydalanish huquqini avtorizasiyalash uchun zarur bo‘lgan texnologiyalar ko‘rsatiladi.
- *Tizimga qaratilgan xavfsizlik siyosatlari (System-Specific Security Policies, SSSP):* mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi. Bunda tashkilotlar tizimni madadlash maqsadida muolajalar va standartlarni o‘z ichiga olgan SSSP siyosatini ishlab chiqadilar va boshqaradilar. Bundan tashqari, tashkilot tomonidan foydalanilgan texnologiyalar tizimga qaratilgan siyosatlarni o‘z ichiga oladi. Bu siyosat texnologiyani amalga oshirish, sozlash va foydalanuvchilar harakatlarini hisobga olishi mumkin.

Tashkilotlarda turli maqsadlarga qaratilgan ko‘plab xavfsizlik siyosatlari mavjud bo‘lishi mumkin. Quyida ularning ayrimlari keltirilgan.

Internetdan foydalanish siyosati. Mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi. Internetdan foydalanish siyosati o‘z ichiga Internetdan foydalanish ruxsati, tizim xavfsizligi, tarmoqni o‘rnatish, AT xizmati va boshqa yo‘riqnomalarni qamrab oladi.

Internetdan foydalanish siyosatini quyidagi to‘rtta kategoriyaga ajratish mumkin:

1. *Tartibsiz siyosat (Promiscuous Policy):* ushbu siyosat tizim resurslaridan foydalanishda hech qanday cheklovlarni amalga oshirmaydi. Masalan, bu siyosatga ko‘ra foydalanuvchi istalgan saytga kirishi, istalgan dasturni yuklab olishi, masofadagi kompyuterdan yoki tarmoqdan foydalanishi mumkin. Bu siyosat korporativ tashkilotlarning ofislarida ishlovchi yoki tashkilotga kelgan mehmonlar uchun foydali hisoblansada, kompyuterni zararli dasturlar asosidagi tahdidlarga zaif qilib qo‘yishi mumkin. Ya’ni, Internetdan foydalanishda cheklanishlar mavjud bo‘lmagani bois, foydalanuvchilar bilimsizligi natijasida zararli dasturlar kirib kelishi mumkin.

2. *Ruxsat berishga asoslangan siyosat (Permissive Policy):* Bu siyosatga ko‘ra faqat xavfli xizmatlar/ hujumlar yoki harakatlar blokirovkalanadi. Masalan, ruxsat berishga asoslangan Internet siyosatida qator keng tarqalgan zararli xizmatlar/ hujumlardan tashqari Internet trafigining asosiy qismi ochiq bo‘ladi. Faqat keng tarqalgan hujumlar va zararli dasturlar blokirovkalanganligi tufayli, ma’mur joriy holatdagi zararli harakatlarga qarshi himoyani ta’minlay oladi. Bu siyosatda har doim yangi hujumlarni va zararli dasturiy ta’minotlarni tutish va bazaga kiritib borish talab etiladi.

3. *Paranoid siyosati (Paranoid Policy):* Paranoid siyosatga ko‘ra barcha narsa blokirovkalanadi va tizim yoki tarmoqdan foydalanuvchi tashkilot kompyuterlarida qat’iy cheklovlar mavjud bo‘ladi. Bu siyosatga ko‘ra foydalanuvchi Internetga umuman ulanmagan yoki qat’iy cheklovlar bilan ulangan bo‘lishi mumkin. Bunday hollarda, foydalanuvchilar odatda siyosatdagi qoidalarni aylanib o‘tishga harakat qiladilar.

4. *Ehtiyotkorlik siyosati (Prudent Policy):* Ehtiyotkorlik siyosati barcha xizmatlar blokirovkalanganidan so‘ng amalga oshirilib, unda xavfsiz va zarur xizmatlarga ma’mur tomonidan individual ravishda

ruxsat beriladi. Bu maksimal xavfsizlikni ta’minlab, tizim/ tarmoq faoliyatiga oid barcha hodisalarni qaydlaydi.

Maqbul foydalanish siyosati. Maqbul foydalanish siyosati tarmoq va web sayt egalari tomonidan qaror qilingan qoidalardan iborat va u hisoblash resurslaridan to‘g‘ri foydalanishni belgilaydi. Ushbu siyosatda foydalanuvchilarning o‘z akkauntlarida mavjud bo‘lgan ma’lumotlarni himoya qilish majburiyati ko‘rsatilgan bo‘lib, foydalanuvchidan tarmoqdan yoki Internetdagi kompyuterdan foydalanishida siyosat cheklovlarini qabul qilishi talab etiladi. Ehtiyotkorlik siyosati prinsiplar, taqiqlar, qayta ko‘rib chiqish va jazo choralarini o‘z ichiga olib, foydalanuvchini, shaxsiy sabablarga ko‘ra, korporativ resurslardan foydalanishini taqiqlaydi.

Maqbul foydalanish siyosati axborot xavfsizligi siyosatining ajralmas qismi hisoblanadi. Bunda, tashkilotlar, o‘zlarining yangi xodimlariga axborot resurlaridan foydalanishga ruxsat berishdan oldin, maqbul foydalanish siyosati bo‘yicha tanishganligi xususida kafolat imzosi olinadi. Maqbul foydalanish siyosati foydalanuvchilarni axborot texnologiyalari infrastrukturasida nimalarni bajarish kerak va nimalarni bajarmaslik kerakligi haqidagi asosiy jihatlarni o‘z ichiga oladi.

Maqbul foydalanish siyosati to‘g‘ri amalga oshirilganiga ishonch hosil qilish uchun ma’mur doimiy ravishda xavfsizlik auditini olib borishi kerak. Masalan, aksariyat tashkilotlar o‘z saytlarida va pochtalarida siyosatga aloqador va diniy mavzularda muzokaralar olib borilishini taqiqlaydi. Maqbul foydalanish siyosatlarining aksariyatida siyosatni buzganlik uchun jazolar tayinlanadi. Bunday jazolar foydalanuvchi akkauntini vaqtincha yopib qo‘yishdan tortib qonuniy jazo choralarigacha bo‘lishi mumkin.

Nazorat savollari

1. Axborot xavfsizligi arxitekturasi va uning sathlari mohiyati.
2. Axborot xavfsizligi strategiyasi tushunchasi.
3. Korxona arxitekturasini tuzishda xavfsizlik strategiyasi va arxitekturasining o‘rni.
4. Axborot xavfsizligi siyosati va uning asosiy vazifasi nimadan iborat?
5. Xavfsizlik siyosati nima uchun zarur?
6. Xavfsizlik siyosatining tarkibi va tuzilishi.
7. Xavfsizlik siyosatining asosiy turlari.
8. Internetdan foydalanish siyosati.

3.BOB. FOYDALANUVCHANLIKNI TA’MINLASH USULLARI

3.1.Foydalanuvchanlik tushunchasi va zaxira nusxalash

Foydalanuvchanlik. Kompyuter xavfsizligi axborot va axborot tizimlarini ruxsatsiz foydalanish, ochish, buzish, o‘zgartirish yoki yo‘q qilishdan himoya qilishni anglatib, uning eng muhim maqsadi axborot konfidensialligini, yaxlitligini va foydalanuvchanligini ta’minlashdir. Kompyuter tizimlaridan ma’lumotlarni saqlash va ishlash uchun foydalanilsa, xavfsizlikni nazoratlash vositalari ma’lumotlarning suiste’mol qilinishidan himoyalashda ishlatiladi. O‘z navbatida, axborot tizimlarining o‘z maqsadiga erishishiga imkon beruvchi foydalanuvchanlikni ta’minlash muhim hisoblanadi.

Foydalanuvchanlik tushunchasiga turli soha korxonalari va olimlar tomonidan turlicha ta’riflar keltirilgan, xususan:

- konfidensial ma’lumotlarga yoki manbalarga ehtiyoji bo‘lganlar uchun foydalanish imkonini berish;
- vakolatli foydalanuvchilarning ma’lumotlardan va axborot tizimlaridan o‘z vaqtida va ishonchli foydalanish imkoniyati;
- obyektlardan qonuniy foydalanish imkoniga ega vakolatli shaxslarning tizimga kirishiga to‘sqinlik qilmaslik;
- tizimlarning tezkor ishlashini va qonuniy foydalanuvchilarga rad etilmaslikni kafolatlash.

Hozirda barcha sohalarda axborot texnologiyalarining keng joriy qilinishi tashkilot yoki korxonalar faoliyatini yuritishda muhim ahamiyat kasb etayotgan bo‘lsada, tashkilotda axborot tizimlari bilan bog‘liq muammo kuzatilsa, uning faoliyati katta yo‘qotishlarga duch kelishi mumkin. Faraz qilaylik, xosting provayderlarida xizmat ko‘rsatishda 99% foydalanuvchanlik ta’minlangan bo‘lsin. Bu qiymat ko‘rinishdan katta bo‘lsada, bir yilda 87 soat (3.62 kun) xizmat ko‘rsatilmaganligini anglatadi. Bu vaqt ichida tashkilot, xizmat ko‘rsatish hajmiga bog‘liq, turlicha zarar ko‘rgan bo‘lishi mumkin. Yuqoridagi holda, hattoki 99.9% xizmat ko‘rsatishda foydalanuvchanlikka erishilgan bo‘lsada, yiliga9 soat yo‘qotish kuzatiladi.

Xizmat ko‘rsatishdagi mazkur zararlarni kamaytirish nafaqat Facebook yoki Amazon kabi yirik korporasiyalar uchun, balki barcha tashkilotlar uchun ham muhim hisoblanadi. Xususan, 2013 yilda 30daqiqa davomida www.amazon.com saytining ishlamay qolishikompaniyaga 2 million dollarga (daqiqasiga 66 240 $) tushgan.

Yuqoridagi misollar har bir tashkilot uchun foydalanuvchanlikni ta’minlash qanchalik muhimligini anglatadi. Yuqori foydalanuvchanlik o‘zida quyidagi 3 ta omilni birlashtiradi:

- *xatolarga bardoshlilik:* bu omil tizimda xatolik kuzatilgan taqdirda ham ishlamay qolmaslik shartini ko‘rsatadi;
- *taqdim etilayotgan xizmatlarning kafolati:* xizmatlar, shuningdek, tizimlar ham har doim mavjud bo‘lishi kerak;
- *ma’lumotlar xavfsizligi:* infrastruktura tarkibidagi ma’lumotlar yaxlitligi, undagi jarayonlar va xodimlar ishlamay qolgan taqdirda ham ta’minlanishi shart.

Yuqori darajadagi foydalanuvchanlik o‘zida birorta ham xatolikni qamrab olmaydi. Boshqacha aytganda, hosting provayderlarining yuqori foydalanuvchanlikni ta’minlashi uchun o‘zidagi biror tarmoq qurilmasi (masalan, marshrutizator yoki tarmoqlararo ekran) ishlamay qolishini oldini olish talab etiladi.

Tizim yoki xizmat foydalanuvchanligini buzilishiga olib keluvchi hujum – *xizmat ko‘rsatishdan voz kechishga undash (DoS)* hujumi hisoblanib, mazkur hujumning asosiy maqsadi tizim yoki tarmoqni qonuniy foydalanuvchilar uchun xizmat ko‘rsatishini to‘xtatishidan iborat. Ushbu hujum turli usul va vositalardan foydalanilib, turli tizim va muhit xususiyati asosida amalga oshiriladi.

Xizmat ko‘rsatishdan voz kechishga undash hujumini oldini olish va foydalanuvchanlikni ta’minlash uchun kompleks himoya choralarini ko‘rish tavsiya etiladi.

Zaxira nusxalash. Hozirgi kunda ma’lumotlarning yo‘qolishi tashkilotlar uchun asosiy xavfsizlik muammolaridan biri bo‘lib, buning natijasida tashkilot katta zarar ko‘rishi mumkin. Shuning uchun, tashkilotdan muhim ma’lumotlarni muntazam zaxira nusxalab borishtalab etiladi.

Ma’lumotlarni zaxira nusxalash – muhim ma’lumotlarni nusxalash yoki saqlash jarayoni bo‘lib, ma’lumot yo‘qolgan vaqtda qayta tiklash imkoniyatini beradi. Ma’lumotlarni zaxira nusxalashdan asosiy maqsad quyidagilar:

– zarar yetkazilganidan so‘ng tizimni normal ish holatiga qaytarish;

– tizimda saqlanuvchi muhim ma’lumotlarni yo‘qolganidan so‘ng uni qayta tiklash.

Tashkilotlarda ma’lumotlar yo‘qolishi moliyaviy tomondan va mijozlarga aloqador holda ta’sir qilishi bilan xarakterlansa, shaxsiy

kompyuterda esa shaxsiy fayllarni, rasmlarni va boshqa qimmatli ma’lumotlarni yo‘qolishiga sababchi bo‘ladi.

Ma’lumotlarni yo‘qolishiga quyidagilar sababchi bo‘lishi mumkin:

- *Inson xatosi:* qasddan yoki tasodifan ma’lumotlarning o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmaganligi yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
- *G‘arazli hatti-harakatlar:* tashkilotdagi muhim ma’lumotlarning modifikatsiyalanishi yoki o‘g‘irlanishi.
- *Tabiiy sabablar:* energiyaning o‘chishi, dasturiy ta’minotning tasodifiy o‘zgarishi yoki qurilmaning zararlanishi.
- *Tabiy ofatlar:* zilzila, yong‘in va h.

Tashkilotda yoki shaxsiy kompyuterda ma’lumotlarni zaxira nusxalash quyidagi imkoniyatlarni taqdim etadi:

- muhim ma’lumotlardan yo‘qolgan va zararlangan taqdirda ham foydalanish;
- tashkilotlarni o‘z faoliyatining to‘xtatilishidan himoyalash va ma’lumotlarni ixtiyoriy vaqtda tiklash;
- tashkilotdagi yo‘qolgan ma’lumotlarni tiklash.

Ma’lumotlarni zaxira nusxalashning ideal strategiyasi ma’lumotni to‘g‘ri tanlashdan boshlab, to ma’lumotni kafolatli tiklash jarayonigacha bo‘lgan bosqichlarni o‘z ichiga oladi. Turli tashkilotlarda zaxiranusxalash farq qilsada, ma’lumotlarni zaxira nusxalashdan oldin quyidagi hususiyatlarga e’tibor qaratish muhim hisoblanadi:

- ma’lumotlarni zaxira nusxalash strategiyasi ixtiyoriy tashqi qurilmalardan ma’lumotlarni tiklash imkoniyatiga ega bo‘lishi shart. Ushbu qurilmalarga misol sifatida serverlar, host mashinalar, noutbuklar va boshqalarni ko‘rsatish mumkin.
- agar tabiiy ofat natijasida ma’lumot yo‘qolsa, zaxira nusxalash strategiyasi faqat chekli sondagi insidentlarga qarshi himoya bilan cheklanmasligi zarur. Tabiiy ofat yuz bergan taqdirda ham strategiya o‘zida ma’lumotlarni tiklash usullarini mujassamlashtirishi shart;
- strategiya dastlabki bosqichlarda ma’lumotlarni qayta tiklash uchun muhim qadamlardan iborat bo‘lishi kerak;
- zaxira nusxalash narxining qimmat bo‘lmasligi tashkilot uchun moliyaviy madad hisoblanadi;
- inson tomonidan bo‘lishi mumkin bo‘lgan xatoliklarni tezlik bilan oldini olish uchun ma’lumotlarni zaxira nusxalash avtomatik tarzda amalga oshirilishi kerak.

Tashkilotlarda zaxira nusxalarni saqlovchilarni tanlash umumiy muammolardan biri hisoblanib, mos bo‘lmagan zaxira saqlovchi vositaning tanlanishi ma’lumotlarning sirqib chiqishiga olib kelishi mumkin. Zaxira nusxalar saqlanuvchi vositalarni tanlash saqlanuvchi ma’lumotlarning turiga bog‘liq va quyidagi omillarga asoslanadi:

- *Narx:* har bir tashkilot o‘zining byudjetiga mos zaxira nusxalash vositasiga ega bo‘lishi shart. Saqlanuvchi ma’lumotlar hajmidan katta hajmga ega vositalarga ega bo‘lish ortiqcha sarf xarajatni keltirib chiqaradi.
- *Ishonchlilik:* tashkilotlar o‘z ma’lumotlarini buzilishsiz ishlaydigan zaxira saqlash vositalarida saqlanishiga erishishlari kerak.
- *Tezlik:* tashkilotlar zaxira nusxalash jarayonida inson aralashuvini imkoni boricha kam talab etadigan saqlash vositalarini tanlashlari kerak.
- *Foydalanuvchanlik:* ma’lumot yo‘qolganidan yoki zararlanganidan so‘ng zaxira nusxalash vositasidan foydalanishda muammolar bo‘lishi mumkin. Shuning uchun, tashkilotlar zaxira nusxalash vositalarining doimo foydalanishga yaroqli bo‘lishiga e’tibor qaratishlari kerak.
- *Qulaylik:* tashkilot foydalanish uchun qulay zaxira nusxalash vositasini tanlashi shart. Bu, o‘z navbatida, zaxira nusxalash jarayonida moslashuvchanlikni ta’minlashda muhim hisoblanadi.

Hozirda ma’lumotlarni zaxira nusxalarini saqlashda quyidagi vositalardan foydalanilmoqda:

Optik disklar (DVD, Blu-ray). DVD disklar 8.55 GBaytgacha ma’lumotlarni saqlash imkoniyatiga ega bo‘lib, ularda faqat o‘qish imkoniyati mavjud. Ushbu ma’lumot saqlagichlarining afzalligi narxining pastligi va foydalanishdagi qulayligi bilan asoslansa, katta hajmdagi ma’lumotlarni saqlay olmasligi uning kamchiligi hisoblanadi.

Ko‘chma qattiq disklar/ USB xotiralar. Ko‘chma qattiq disklar DVD, Blu-ray disklarga qaraganda kichikroq hajmli zaxira ma’lumotlarini saqlash uchun yaxshi vosita hisoblanadi. Flesh disklar esa turli o‘lchamli bo‘lib, katta hajmdagi ma’lumotlarni ham saqlash imkoniyatiga ega. Qattiq disklardan foydalanishning yana bir varianti – RAID (Redundant Array of Independent Disks) hisoblanadi.

Lentali disklar. Lentali disklar ma’lumotlarni zaxira saqlash uchun eng mos saqlagichlar bo‘lib, tashkilot sathida ma’lumotni zaxira nusxalashni amalga oshiradi. Ushbu saqlagichlardan ma’lumotlarni va dasturlarni saqlash uchun foydalaniladi. Ushbu zaxira saqlagichi olib

yurish uchun qulay, foydalanuvchi ishtirokini talab etmaydi va to‘liq avtomatlashgan tarzda amalga oshiriladi. Uning asosiy kamchiligi oddiy foydalanuvchilar uchun qimmatligi va oddiy kompyuterlardan foydalanishi uchun qo‘shimcha apparat va dasturiy vositani talab qilishi.

3.2.Ma’lumotlarni zaxiralash texnologiyalari va usullari

Aksariyat tashkilotlar muhim ma’lumotlarini RAID texnologiyasi asosida zaxira nusxalashni amalga oshiradilar. RAID texnologiyasida ma’lumotlar bir qancha disklarning turli sohalarida saqlangani bois, IO (kirish/ chiqish) amallarining bajarilishi osonlashadi. RAID texnologiyasi ko‘plab qattiq disklarni bitta mantiqiy disk sifatida o‘rnatish orqali ishlaydi. Ushbu texnologiya disklar massivi bo‘ylab bir xil ma’lumotlarni muvozanatlashgan shaklda saqlash imkoniyatini beradi. Ushbu texnologiya odatda serverlarda ma’lumotlarni saqlashga mo‘ljallangan, shaxsiy kompyuterlardan foydalanish zaruriyati mavjud emas.

RAID texnologiyasida amallarni samarali bajarish uchun 6 ta sath mavjud: RAID 0, RAID 1, RAID 3, RAID 5, RAID 10 va RAID 50. RAIDning har bir sathi quyidagi xususiyatlarga ega:

- *xatoga bardoshlilik:* agar biror disk ishlashdan to‘xtasa, boshqa disklar normal ishlashini davom ettiradi;
- *unumdorlik:* RAID ko‘plab disklar bo‘ylab o‘qish va yozishda yuqori unumdorlik darajasiga ega.

Disklarning ma’lumotlarni saqlash imkoniyati mos RAID sathini tanlashga asoslanadi. Saqlash hajmi individual RAID disklar o‘lchamining bir xil bo‘lishini talab etmaydi. Barcha RAID sathlari quyidagi saqlash usullariga asoslanadi:

- *bloklash:* ma’lumotlar ko‘plab bloklarga ajratiladi. Mazkur bloklar keyinchalik RAID tizimi orqali yoziladi. Bloklash ma’lumotlarni saqlanishini yaxshilaydi.
- *akslantirish:* akslantirish ma’lumotlarning nusxalanishini va RAID bo‘ylab uzluksiz saqlanishini amalga oshiradi. Bu usul xatoga bardoshli va amalga oshirilishining yuqori darajasiga ega.
- *nazorat qiymati:* nazorat qiymati ma’lumotlar bloki yaxlitligini ekshirish funksiyasini amalga oshirishda bloklash funksiyasidan foydalanadi. Disk buzilganida nazorat qiymati xatolikni tuzatish funksiyasi yordamida ma’lumotlarni tiklashga harakat qiladi.

RAID tizimlari sathga bog‘liq holda o‘ziga xos afzalliklar va kamchiliklarga ega.

RAID tizimlarining afzalliklari:

Unumdorlik va ishonchlilik: RAID texnologiyasi disklarda ma’lumotlarni o‘qish va yozish unumdorligini oshiradi. Ushbu texnologiya IO jarayonini taqsimlash orqali unumdorlikni yaxshilaydi va jarayon tezligi, yagona diskda ma’lumotlarni saqlashga qaraganda, yuqori bo‘ladi.

Xatolikni nazoratlash: buzilgan diskda saqlangan ma’lumotlarni qolgan diskdagi ma’lumotlar bilan taqqoslash orqali ularni tiklashni yoki tuzatishni amalga oshiradi.

Ma’lumotlar ortiqchaligi (ma’lumotlarni nusxalash): diskning buzilishi istalgan vaqtda yuzaga kelishi mumkin. RAID texnologiyasi qurilma buzilganida ma’lumotlarni nusxalash orqali uning qayta tiklanishini ta’minlaydi.

Disklarni navbatlanishi: ma’lumotlarni o‘qish/ yozish unumdorligini oshiradi. Ma’lumotlar kichik bo‘laklarga bo‘linib, bir qancha disklar bo‘ylab tarqatiladi. RAID tizimida ma’lumotlarni o‘qish va yozish bir vaqtda bajariladi.

Tizimning ishlash davomiyligi: ushbu o‘lchov kompyuterning ishonchligini va barqarorligini belgilaydi. Tizimning ishlash davomiyligi tizimning avtomatik ishlash vaqtini belgilaydi.

RAID tizimlarining kamchiliklari:

Tarmoq drayverlarini yozish: RAID texnologiyasi asosan serverlarda foydalanish uchun loyihalangani bois, uning asosiy kamchiligi - barcha tarmoq drayverlarini yozish.

Mos kelmaslik: tizimlar turli RAID drayverlarini madadlaydi. Muayyan apparat yoki dasturiy komponent serverda sozlangan RAID tizimi bilan mos kelmasligi mumkin. Mos kelmaslik RAID tizimining o‘z vazifasini to‘g‘ri amalga oshirilmasligiga olib kelishi mumkin.

Ma’lumotlarning yo‘qolishi: RAID drayverlari mexanik muammolar tufayli o‘z funksiyalarini bajara olmasliklari mumkin. Disklar ketma-ket buzilishga uchraganida ma’lumotlarning yo‘qolishi xavfi ortadi.

Qayta tiklashning uzoq vaqti: katta hajmli disklardan foydalanish ma’lumotlarni uzatish tezligini ortishiga olib keladi. Biroq, katta hajmli disklarda ma’lumotlarni tiklash va buzilgan disklarni qayta sozlash uzoq vaqt talab etadi.

Narxining yuqoriligi: RAID texnologiyasini amalga oshirish iqtisodiy jihatdan katta mablag‘ni talab etadi. Bundan tashqari, tizim

ishini yaxshilash uchun qo‘shimcha RAID kontrollerlarini va qurilma drayverlarini sotib olish talab etiladi.

Mos RAID sathini tanlash tashkilot zaruriyatidan kelib chiqqan holda va har bir sathning taqdim qilayotgan imkoniyatlariga asoslanishi zarur. RAID sathini tanlashda ularni xususiyatlariga ham e’tibor berish talab etiladi (6.1-jadval).

3.1-jadval

RAID texnologiyalarining tahlili

RAID	**Diskdan foydalanish**	**Buzilishga bardoshligi**	**Katta ma’lumotlar transferi**	**IO darajasi**	**Ma’lumot foydalanuvchanligi**	**Asosiy kamchiligi**
Yagona disk	Bir xil 100%	Yo‘q	Yaxshi	Yaxshi	Yagona diskning MTBF davri	Disk buzilsa, ma’lumot yo‘qoladi
RAID 0	A’lo 100%	Ha	Juda yaxshi	Juda yaxshi	Diskning past MTBF davri	
RAID 1	O‘rtacha 50%	Ha	Yaxshi	Yaxshi	Yaxshi	Disk hajmidan 2 marta kam foydalanish
RAID 3	Yaxshi-juda yaxshi	Ha	Juda yaxshi	Yaxshi	Yaxshi	Disk buzilsa, ma’lumot yo‘qoladi
RAID 5	Yaxshi-juda yaxshi	Ha	Yaxshi-juda yaxshi	Yaxshi	Yaxshi	Disk buzilsa, kam o‘tkazuvchanlik
RAID 0+1	O‘rtacha 50%	Ha	Yaxshi	Juda yaxshi	Yaxshi	Disk hajmidan 2 marta kam foydalanish
RAID 1+0	O‘rtacha 50%	Ha	Juda yaxshi	Juda yaxshi	Juda yaxshi	Juda qimmat, keng ko‘lamli emas
RAID 30	Yaxshi-juda yaxshi	Ha	Juda yaxshi	A’lo	A’lo	Juda qimmat
RAID 50	Yaxshi-juda yaxshi	Ha	Yaxshi-juda yaxshi	A’lo	A’lo	Juda qimmat

Izoh: MTBF – Mean Time Between Failures (buzilishlar o‘rtasidagi o‘rtacha vaqt).

Zaxira nusxalash usullari. Tashkilot o‘zining moliyaviy imkoniyati va AT infrastrukturasi asosida zaxira nusxalash usulini tanlaydi. Ma’lumotlarni zaxira nusxalashning quyidagi usullari mavjud.

Issiq zaxiralash. Ma’lumotlarni zaxira nusxalashning mazkur usuli amalda keng qo‘llaniladi va dinamik yoki aktiv zaxira nusxalash usuli deb ham ataladi. Ushbu usulga binoan foydalanuvchi tizimni boshqarayotgan vaqtida zaxira nusxalash jarayonini ham amalga oshirishi mumkin. Mazkur zaxiralash usulini amalga oshirish tizimning harakatsiz vaqtini kamaytiradi. Zaxiralash davomida ma’lumotlardagi o‘zgarish yakuniy zaxira nusxasiga ta’sir qilmaydi. Ravshanki, zaxiralashni amalga oshirish vaqtida tizimning ishlash jarayoni sekinlashadi.

Sovuq zaxiralash. Ushbu zaxiralash usuli offlayn zaxiralash deb ham atalib, tizim ishlamay turganida yoki foydalanuvchi tomonidan boshqarilmagan vaqtda amalga oshiriladi. Ushbu usul zaxiralashning xavfsiz usuli bo‘lib, ma’lumotlarni nusxalashda turli tahdidlardan himoyalaydi.

Iliq zaxiralash. Ushbu zaxiralashda tizim muntazam yangilanishni amalga oshirish uchun tarmoqqa bog‘lanishi kerak bo‘ladi. Bu ma’lumotlarni akslantirish yoki nusxalash hollarida muhim hisoblanadi. Ushbu usulda ma’lumotlarni zaxiralash uzoq vaqt oladi va jarayon biror vaqt intervalida amalga oshiriladi (kundan xaftagacha).

Zaxira nusxalashda ma’lumotlarni saqlash manzilini tanlash muhim hisoblanadi. Zaxira nusxalarni quyidagi manzillarda saqlash mumkin.

Ichki (onsite) zaxiralash. Ushbu zaxiralash usuli tashkilot ichida amalga oshirilib, tashqi qurilmalar, lentali saqlagichlar, DVD, qattiq disk va boshqa saqlagichlardan foydalaniladi. Ichki zaxiralash qurilmalari zaxira saqlanuvchi ma’lumotlar hajmiga muvofiq tanlanadi.

Tashqi (offsite) zaxiralash. Tashqi zaxiralash mosofadagi manzilda amalga oshirilib, fizik disklarda ma’lumotlarni saqlash onlayn yoki uchinchi tomon xizmati orqali amalga oshirilishi mumkin.

Bulutli tizimda zaxiralash. Ushbu zaxiralash usuli onlayn usuli deb ham ataladi. U zaxiralangan ma’lumotlarni ochiq tarmoqda yoki ma’lum serverda saqlaydi. Odatda ma’lum server vazifasini uchinchi tomon xizmati amalga oshirishi mumkin.

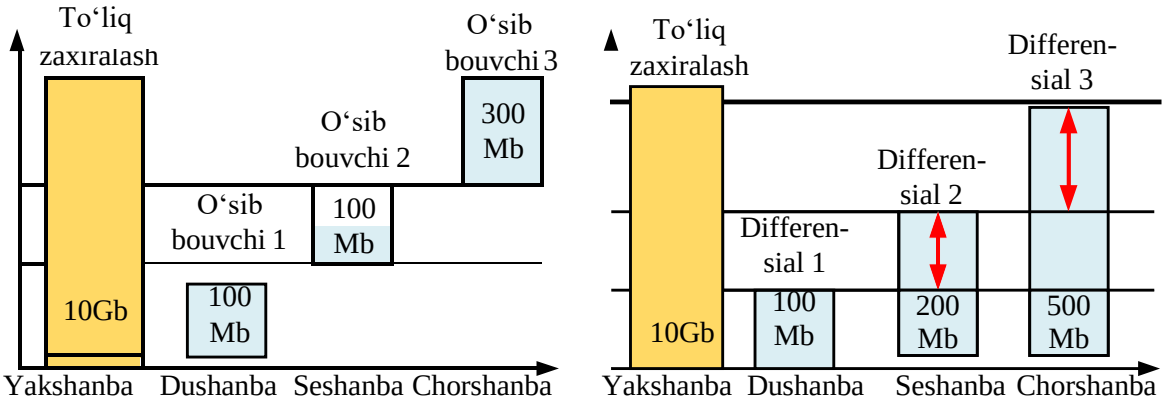
Zaxiralash turlari. Mos zaxiralash turi tarmoqqa ortiqcha yuklama qo‘shmaydi hamda narx, vaqt va resursni kam talab qiladi. Amalda uchta turdagi zaxiralash turlari mavjud: *to‘liq, differensial* va *o‘sib boruvchi*.

To‘liq zaxiralash: ushbu usul normal zaxiralash deb ham atalib, jadvalga ko‘ra avtomatik tarzda amalga oshiriladi. Bunda, barcha fayllar

nusxalanadi va zichlangan tarzda saqlanadi. Ushbu usul nusxalangan ma’lumotlar uchun samarali himoyani ta’minlaydi.

O‘sib boruvchi zaxiralash: ushbu usulga ko‘ra zaxiralanuvchi ma’lumotlarga nisbatan o‘zgarish yuz berganida zaxiralash amalga oshiriladi. Oxirgi zaxira nusxalash sifatida ixtiyoriy zaxiralash usulidan foydalanish mumkin. Shuning uchun, o‘sib boruvchi zaxiralashni amalga oshirishdan oldin, tizim to‘liq zaxiralashni amalga oshirishi shart.

Faraz qilaylik, zaxira nusxalash jadvaliga ko‘ra to‘liq zaxiralash yakshanba kuniga, ortib boruvchi zaxiralash esa seshanbadan shanbagacha amalga oshirilishi belgilangan bo‘lsin. Yakshanba kuni to‘liq zaxiralash amalga oshirilganidan so‘ng, dushanba kunidagi o‘zgarishlar seshanba kuni o‘sib boruvchi usul asosida amalga oshiriladi. Ushbu jarayoni shanbagacha davom ettiriladi (6.1 – rasm “a”).



a) O‘sib boruvchi zaxiralash

b) Differensial zaxiralash

3.1-rasm. Zaxiralash turlari

Differensial zaxiralash: ushbu zaxiralash usuli to‘liq va o‘sib boruvchi usullarning mujassamlashgan ko‘rinishi bo‘lib, oxirgi zaxiralangan nusxadan boshlab bo‘lgan o‘zgarishlarni zaxira nusxalash amalga oshiriladi.

Masalan, yuqoridagi misolni qaraylik. To‘liq zaxiralash yakshanba kuni, differensial nusxalash esa shanbagacha amalga oshirilishi jadvalda keltirilgan bo‘lsin. Yakshanba kuni to‘liq zaxira nusxalash amalga oshirilganidan so‘ng, dushanba kuni differensial zaxiralash kun o‘tishi bilan amalga oshiriladi. Bu holat o‘sib boruvchi zaxiralashga o‘xshab ketadi. Biroq, seshanbada, zaxira nusxalash yakshanba va dushanbadagi o‘zgarishlar uchun amalga oshiriladi. Shundan so‘ng, chorshanbada zaxiralash yakshanba, dushanba va seshanba kunlari uchun amalga oshiriladi (6.1 – rasm “b”).

3.3.Ma’lumotlarni qayta tiklash va hodisalarni qaydlash

Ma’lumotlarni qayta tiklash. Ma’lumotlarning yo‘qolishi har qanday tashkilot uchun jiddiy muammo hisoblanadi. Shu sababli, ma’lumotlarni qayta tiklash usullaridan foydalanish talab etiladi. Ushbu jarayon ma’lumotlarning qanday yo‘qolganiga, ma’lumotlarni qayta tiklash dasturiy vositasiga va ma’lumotlarni tiklash manziliga bog‘liq.

Ma’lumotlarni eltish vositalarida, USB xotirada, qattiq diskda, DVD va boshqa saqlagichlarda ma’lumotlarni qayta tiklash mumkin. Qayta tiklash jarayonining muvaffaqqiyatli amalga oshirilishi foydalanuvchining malakasiga bog‘liq. Ma’lumotlarni qayta tiklash jarayonida bilim va to‘g‘ri tanlangan vosita muhim hisoblanadi.

Ma’lumotlarni qayta tiklash har doim ham muvaffaqiyatli bo‘lmasligi mumkin. Agar saqlagichda xatolik mavjud bo‘lsa yoki unga ko‘p zarar yetgan bo‘lsa, ma’lumotlarni tiklashning imkoni bo‘lmasligi mumkin. Ma’lumotlarning qayta tiklanishi ehtimoli ularning yo‘qolishi sababiga bog‘liq. Ma’lumotlarni yo‘qolishiga sabab bo‘luvchi hollar quyidagilar:

Faylni o‘chirish: agar fayl o‘chirilsa, ushbu soha qaytadan yozilgunga qadar saqlagichda mavjud bo‘ladi. Ma’lumotlar saqlangan sohadagi kichik xotiraga ma’lumotlar yozilishi butun ma’lumotlarni tiklanmasligiga sababchi bo‘lishi mumkin. Windows OTda NTFS fayl tizimida ma’lumotlarni o‘chirish algoritmi mavjud va ma’lumotlarni tiklash ham ushbu algoritm asosida amalga oshiriladi.

Faylning zararlanishi: agar OT zararlansa, ma’lumotlarni diskning qismlar jadvali yordamida tiklash mumkin. Agar diskning qismlar jadvali ham zararlangan bo‘lsa, qayta tiklashning maxsus vositalaridan foydalanishga to‘g‘ri keladi.

Qattiq diskning fizik zararlanishi: qattiq diskka fizik ta’sir bo‘lishi, faylni zararlanishiga qaraganda, katta yo‘qotishlarga sabab bo‘lishi mumkin. Bu esa ma’lumotlarni qayta tiklashning maxsus sathidan foydalanishni talab etadi. Zararlangan fizik diskdan ma’lumotlarni tiklash vaqtida, tiklash jarayonining muhiti turli ifloslanishlardan holi bo‘lishi zarur. Ya’ni, bu jarayon toza xonada amalga oshirilishi shart. Chang bo‘lgan sohalarda ma’lumotlarning qayta tiklanishi qiyin bo‘ladi.

Ma’lumotlarni qayta tiklashda quyidagilarni esda saqlash zarur:

- ma’lumotlar yo‘qolgan qattiq diskga qayta tiklangan ma’lumotlarni yozmaslik;
- turli zaxira nusxalarni amalga oshirish va ularni turli manzillarda saqlash;

- ma’lumotlarni qayta tiklash har doim ham 100% samara bermasligi.

Amalda saqlagichlardagi yo‘qolgan ma’lumotlarni tiklashda maxsus dasturiy vositalardan foydalaniladi. Ularga *Recovery My Files*, *EASEUS Data Recovery Wizard*, Advanced Disk Recovery, Handy Recovery, R-Studio, Data Recovery Pro, Recuva, Total Recall, Pandora Recovery kabilarni misol sifatida keltirish mumkin.

Hodisalarni qaydlash. Xatolik yuz berganida, tizim ma’muri yoki madadlash xodimi xatoning sababini aniqlashi, yo‘qolgan ma’lumotlarni qayta tiklashga urinishi va xatoning takrorlanishiga yo‘l qo‘ymasligi lozim. Ilovalar, operatsion tizim va boshqa tizim xizmatlari muhim voqealarni, masalan, xotira hajmining kamligi yoki diskdan foydalanishga haddan tashqari ko‘p urinishlarni qayd etishi muhim hisoblanadi. Keyinchalik tizim ma’muri xato sababini aniqlashi va u sodir bo‘lgan kontekstni aniqlash uchun hodisalar jurnalidan (log fayl deb ataladi) foydalanishi mumkin.

Hodisalarni qaydlash quyidagilarni o‘z ichiga olishi shart:

operatsion tizim hodisalari:

– tizimni ishga tushirish va o‘chirish;

– xizmatni boshlash va tugatish;

– tarmoq ulanishidagi o‘zgarishlar yoki muvaffaqiyatsizliklar;

– tizim xavfsizligini sozlash va boshqarish vositalarini o‘zgartirishga urinishlar.

OT audit yozuvlari:

– tizimga kirishdagi urinishlar (muvaffaqiyatli yoki muvaffaqiyatsiz);

– tizimga kirgandan so‘ng bajariladigan funksiyalar (masalan, muhim faylni o‘qish yoki yangilash, dasturni o‘rnatish);

– qayd yozuvini o‘zgartirish (masalan, yozuvni yaratish va yo‘q qilish, imtiyozlarni tayinlash);

– imtiyozli qayd yozuvidan muvaffaqiyatli / muvaffaqiyatsiz foydalanish.

ilova qayd yozuvi to‘g‘risidagi ma’lumot:

– ilovani muvaffaqiyatli va muvaffaqiyatsiz autentifikatsiya qilishga urinishlar;

– hisob qaydnomasidagi o‘zgartirishlar (masalan, qayd yozuvini yaratish va yo‘q qilish, qayd yozuvi imtiyozlarini tayinlash);

– dastur imtiyozlaridan foydalanish.

ilova amallari:

– dasturni ishga tushirish va o‘chirish;
– dastur xatolari;
– dastur konfigurasiyasidagi asosiy o‘zgarishlar.

Har bir hodisa uchun qaydlangan tafsilotlar farqlanadi, ularni quyidagi parametrlar bo‘yicha qaydlash tavsiya qilinadi:

– vaqt belgisi;
– hodisa, holat va / yoki xatolik kodlari;
– servic / buyruq / ilova nomi;
– foydalanuvchi yoki tizim bilan bog‘liq voqea;
– amaldagi qurilma (masalan, IP va manba manzili, terminal sessiyasi identifikatori, web brauzer va h.).

Audit jurnallarida barcha harakatlar qaydlangani bois, niyatibuzuqlar ularni tahrirlash orqali o‘z faoliyatini yashirishi mumkin. Shuning uchun, audit jurnalidan foydalanishlarni nazoratlash muhim vazifa hisoblanadi.

Windows OTda hodisa turlari. Windows OTda besh turdagi hodisa ro‘yxatga olinadi. Bularning barchasi uchun aniq belgilanganma’lumotlar mavjud bo‘lib, biror bir hodisa haqidagi xabar faqat bitta turga tegishli bo‘ladi (6.2-jadval).

3.2-jadval

Windows OT hodisalari turlari

Hodisa	**Tavsifi**
1	**2**
Xatolik	Ma’lumotlarni yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan hodisa. Masalan, biror xizmat ishga tushirishi paytida yuklanmasa, mazkur xatolik hodisasi qayd etiladi.
Ogohlantirish	Hodisa juda ahamiyatli bo‘lmasada, kelajakda yuzaga kelishi mumkin bo‘lgan muammolarni ko‘rsatishi mumkin. Masalan, diskda bo‘sh joy kam bo‘lsa, ogohlantirish hodisasi qayd etiladi.
Axborot	Ilova, drayver yoki xizmatning muvaffaqiyatli ishlashini tavsiflaydigan hodisa. Masalan, tarmoq drayveri muvaffaqiyatli yuklanganida, hodisalarni axborot qaydlaydi.

1	2
Muvaffaqiyatli audit	Muvaffaqiyatli tekshirilgan xavfsizlikka oid kirish urinishlarini yozib boradigan hodisa. Masalan, foydalanuvchining tizimga kirishga muvaffaqiyatli urinishi muvaffaqiyatli audit hodisasi sifatida qaydlanadi.
Muvaffaqiyatsiz audit	Tekshirilgan xavfsizlikdan foydalanishga urinish muvaffaqiyatsiz tugaganida, bu hodisa qaydlanadi. Masalan, agar foydalanuvchi tarmoq drayveriga kirishida muvaffaqiyatsizlikka uchrasa, bu hodisa qaydlanadi.

Quyidagi hodisalar qaydlanishi shart:

Resurs muammolari. Xotirani ajratishda xatolik yuz bergan taqdirda ogohlantirish hodisasini qaydlash kam xotirali vaziyatning sababini ko‘rsatishga yordam beradi.

Uskuna bilan bog‘liq muammolar. Tarmoq kartasi, qattiq disk, tezkor xotira va boshqa qurilma drayveri bilan bog‘liq hodisalar qaydlanishi shart.

Axborot hodisalari. Server dasturi (masalan, ma’lumotlar bazasi serveri) foydalanuvchining ro‘yxatdan o‘tkazilishi, ma’lumotlar bazasidagi amallar va boshqa hodisalar qaydlanishi shart.

Hodisalarni qaydlash jurnali ustida quyidagi amallar bajarilishi mumkin:

- zaxira nusxalash (BackupEventLog funksiyasi yordamida);
- tozalash (ClearEventLog funksiyasi yordamida);
- monitoringlash (NotifyChangeEventLog funksiyasi yordamida);
- so‘rov yuborish (boshqa dasturlar tomonidan, GetOldestEventLogRecord, GetNumberOfEventLogRecords funksiyalari yordamida);
- o‘qish (ReadEventLog funksiyasi yordamida);
- yozish (ReportEvent funksiyasi yordamida).

Windows XP/2000 operatsion tizimlarda hodisalarni qaydlash jurnalida turli qayd yozuvlari uchun berilgan imtiyozlar mavjud (6.3-jadval).

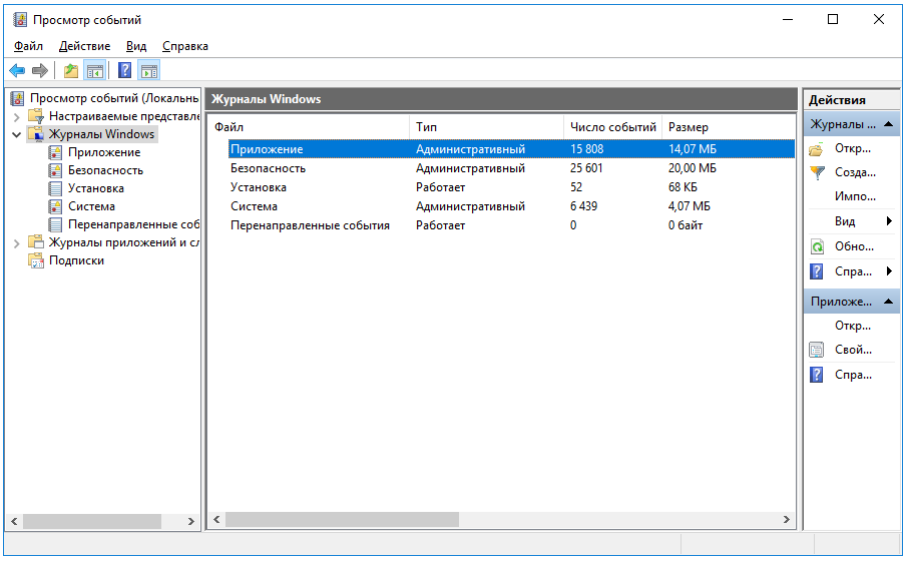
3.3-jadval

Windows XP/2000 operatsion tizimda hodisa jurnalida mavjud imtiyozlar

Log	Qayd yozuvi	O‘qish	Yozish	Tozalash
Ilovaga tegishli	Ma’murlar (tizim)	+	+	+
	Ma’murlar (domen)	+	+	+
	Lokal tizim	+	+	+
	Interaktiv foydalanuvchi	+	+	-
Tizimga tegishli	Ma’murlar (tizim)	+	+	+
	Ma’murlar (domen)	+	-	+
	Lokal tizim	+	+	+
	Interaktiv foydalanuvchi	+	-	-
Tanlovga ko‘ra yaratilgan log fayl	Ma’murlar (tizim)	+	+	+
	Ma’murlar (domen)	+	+	+
	Lokal tizim	+	+	+
	Interaktiv foydalanuvchi	+	+	-

Windows OT da hodisalarni qaydlash fayllarini (log faylni) ko‘rish uchun quyidagi ketma-ketlik amalga oshiriladi:

1. Kompyuterda Win+R tugmalar kombinatsiyasi bosiladi.
2. Hosil bo‘lgan oynadagi maydonda *eventvwr* kiritiladi va Enter tugmasi bosiladi.
3. Hosil bo‘lgan hodisalarni ko‘rish oynasidan *Windows Logs* bandi tanlanadi (6.2-rasm).



3.2-rasm. Windows OTning hodisalar jurnali oynasi

Nazorat savollari

1. Foydalanuvchanlik tushunchasi va uning tizim uchun muhimligi.
2. Zaxira nusxalash va uning turlari.
3. Ma’lumotlarni yo‘qolishiga olib keluvchi asosiy sabablar.
4. Zaxira nusxalashda bajariluvchi vazifalar ketma-ketligi.
5. Zaxira nusxalarni saqlovchi vositalar va ularning xususiyatlari.
6. RAID texnologiyasi va uning asosiy xususiyatlari.
7. Zaxiralash turlari va ularning afzalliklari va kamchiliklari.

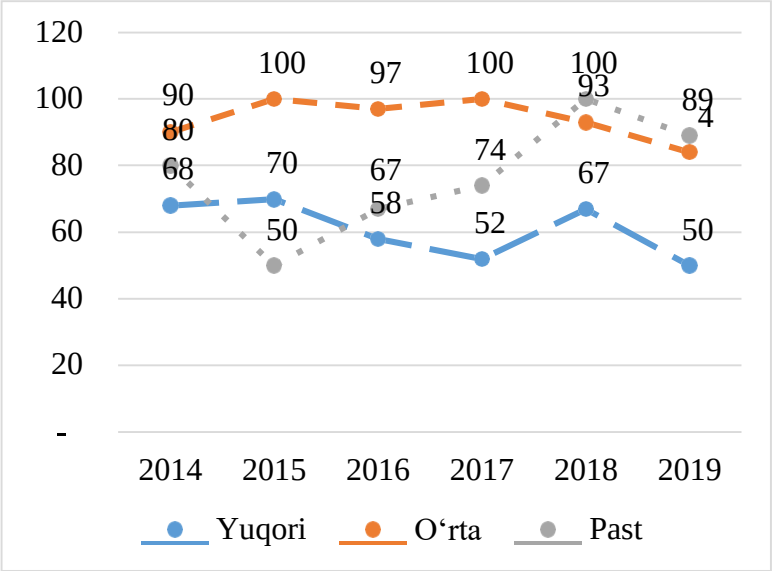
4.BOB. DASTURIY VOSITALAR XAVFSIZLIGI

4.1.Dasturiy vositalardagi xavfsizlik muammolari

Hozirda dasturiy vositalar xavfsizligi axborot xavfsizligining kriptografiya, foydalanishni nazoratlash va xavfsizlik protokollari kabi muhim sohalardan hisoblanadi. Bunga sabab - axborotning virtual xavfsizligi dasturiy vositalar orqali amalga oshirilishi. Dasturiy vosita tahdidga uchragan taqdirda xavfsizlik mexanizmi ham ishdan chiqadi.

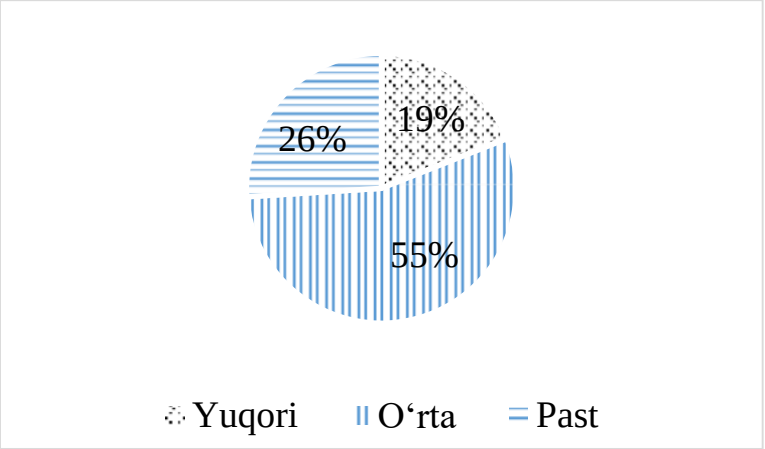
Barcha dasturiy vositalarda zaifliklar mavjud, ularning muhimlik darajalari turlicha. Masalan, narxi 165 mln. $ ni tashkil etgan NASA Mars Lander Mars sayyorasi yuzasiga qo‘nish vaqtida halokatga uchragan. Bunga sabab, oddiy ingliz va xalqaro metr uzunlik o‘lchovlari orasidagi farq bo‘lgan. Bundan tashqari, Denver xalqaro aeroportidagi yuklarni boshqarish tizimida foydalanilgan dasturiy vositadagi kamchilik natijasida 11 oy davomida kuniga 1 mln. $ dan zarar ko‘rilgan.

So‘nggi yillarda ushbu zaiflik muammolarining soni va jiddiylik darajasi ortib bormoqda. Xususan, 7.1-rasmda Positive Technologies tashkiloti tomonidan veb-saytlardagi turli darajadagi zaifliklarni yillar bo‘yicha ortib borishi keltirilgan.



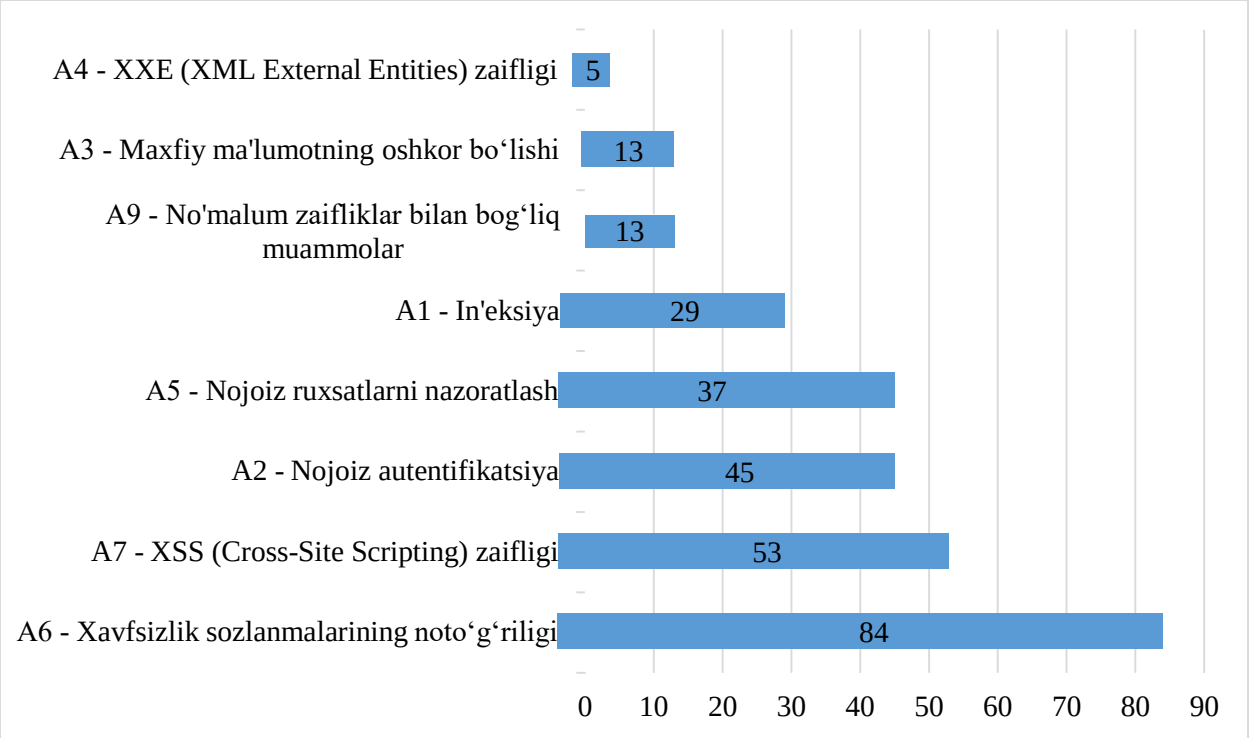
4.1– rasm. Turli darajadagi zaifliklarga ega Web-saytlar soni

2019 yilda aniqlangan web-saytlardagi muammolarning jiddiyligi bo‘yicha taqsimoti 4.2-rasmda keltirilgan.



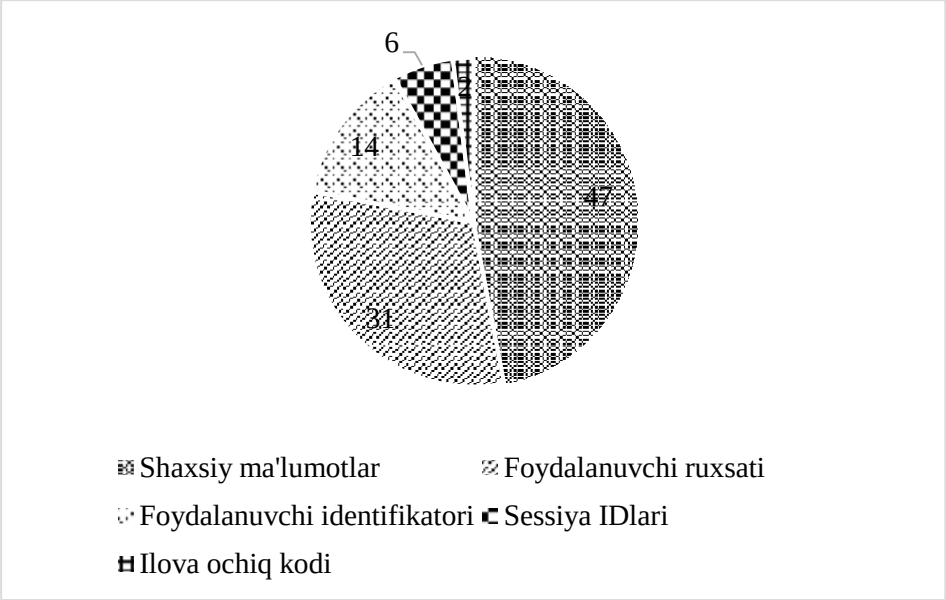
4.2-rasm. Web-sayt muammolarining jiddiyligi bo‘yicha taqsimoti

2019 yilda veb-saytlarda keng tarqalgan zaifliklar va ularning ulushi, OWASP (Open Web Application Security Project) tomonidan berilgan ma’lumotga ko‘ra, quyidagicha bo‘lgan (7.3-rasm).



4.3-rasm. OWASP tashkiloti 2019 yilda uchragan zaifliklar va ularning ulushi

Yuqorida keltirilgan zaifliklar natijasida turli ma’lumotlarni hujumchilar tomonidan qo‘lga kiritish maqsad qilingan (4.4-rasm).



4.4-rasm. Zaifliklar natijasida qo‘lga kiritishga mo‘ljallangan ma’lumotlar

Dasturiy vositalardagi mavjud tahdidlar, odatda, dasturlash tillari imkoniyatlari bilan belgilanadi. Masalan, nisbatan quyi dasturlash tillari dasturchidan yuqori malakani talab etgani bois, ularda ko‘plab xavfsizlik muammolari paydo bo‘ladi. C# va Java dasturlash tillarida ko‘plab muammolar avtomatik tarzda kompilyasiya jarayonida aniqlanganligi sababli, C yoki C++ dasturlash tillariga nisbatan, xavfsiz hisoblanadi.

Odatda zararli dasturiy vositalar ikki turga bo‘linadi:

– dasturlardagi zaifliklar (atayin yaratilmagan);
– zararkunanda dasturlar (atayin yaratilgan).

Birinchi turga, dasturchi tomonidan yo‘l qo‘yilgan xatolik natijasidagi dasturlardagi muammolar misol bo‘lsa, ikkinchi turga buzg‘unchilik maqsadida yozilgan maxsus dasturiy mahsulotlar (masalan, viruslar) misol bo‘la oladi.

Dasturiy vositalarda xavfsizlik muammolarining mavjudligi quyidagi omillar orqali belgilanadi:

– dasturiy vositalarning ko‘plab dasturchilar tomonidan yozilishi (komplekslilik);
– dasturiy mahsulotlar yaratilishida inson ishtiroki;
– dasturchining malakasi yuqori emasligi;
– dasturlash tillarining xavfsiz emasligi.

Dasturiy vositalarning bir necha million qator kodlardan iborat bo‘lishi xavfsizlik muammosini ortishiga sababchi bo‘ladi (7.1-jadval). Boshqacha aytganda, katta hajmli dasturiy vositalar ko‘plab dasturchilar tomonidan yoziladi va yakunida biriktiriladi. Dasturchilar orasidan

bittasining bilim darajasi yetarli bo‘lmasligi, butun dasturiy vositaning xavfsizligini yo‘qqa chiqarishi mumkin.

4.1 – jadval

Turli OTlar kodlarining uzunligi

Tizim	**Dasturdagi kod uzunligi**
Netscape	17 mln.
Space Shuttle	10 mln.
Linuxkernel 2.6.0	5 mln.
Windows XP	40 mln.
Mac OS X 10.4	86 mln.
Boeing 777	7 mln.

Tahlillar natijasi har 10 000 ta qator kodda 5 ta bag mavjudligini ko‘rsatadi. Boshqacha aytganda, o‘rtacha 3kbayt .exe faylda 50 tacha bag bo‘ladi.

Dasturiy vositalar injineriyasida dasturning o‘z vazifasini kafolatli bajarishiga harakat qilinsa, *xavfsiz* dasturiy vositalar injineriyasida esa o‘z vazifasini xavfsiz bajarishi talab etiladi. Biroq, amalda butunlay xavfsiz dasturiy vositaning bo‘lishi mumkin emas.

Dasturiy mahsulotlarda zaiflikka tegishli quyidagi tushunchalar mavjud.

Nuqson. Dasturni amalga oshirishdagi va loyihalashdagi zaifliklarning barchasi nuqson hisoblanadi va uning dasturiy vositalarda mavjudligi yillar davomida bilinmasligi mumkin.

Bag. Baglar dasturiy ta’minotni amalga oshirish bosqichiga tegishli muammo bo‘lib, ularni osongina aniqlash mumkin. Misol sifatida dasturlashdagi *buferning to‘lib-toshishi* (Buffer overflow) holatini keltirish mumkin.

Xotiraning to‘lib-toshishi. Amalda ko‘p uchraydigan dasturlash tillaridagi kamchiliklar, odatda, taqiqlangan formatdagi yoki hajmdagi ma’lumotlarning kiritilishi natijasida kelib chiqadi. Bu turdagi tahdidlar ichida keng tarqalgani – xotiraning to‘lib-toshishi tahdidi.

Masalan, foydalanuvchidan web-saytga ma’lumotlar kiritilishi talab etilsa (ismi, familiyasi, yili va h.), foydalanuvchi tomonidan kiritilgan “ism” maydonidagi ma’lumot serverdagi *N* ta belgi hajmiga ega sohaga yoziladi. Agar kiritilgan ma’lumot uzunligi *N* dan katta bo‘lsa, xotiraning to‘lib-toshishi hodisasi sodir bo‘ladi.

Agar buzg‘unchi tomonidan o‘ziga “kerakli” ma’lumot kiritilsa, bu o‘z navbatida kompyuterning buzilishiga olib keladi.

Quyida C dasturlash tilida yozilgan kod keltirilgan, agar bu kod kompilyasiya qilinsa, xotiraning to‘lib-toshishi hodisasi sodir bo‘ladi.

```
int main()
  {
  int buffer [10];
  buffer [20] =37;
  }
```

Bu yerda mavjud muammo - 10 bayt o‘lchamli xotiraga 20 baytli ma’lumot yozilishi. Bu esa xotiraning ruxsat etilmagan manziliga ham murojaatga sabab bo‘ladi.

4.2.Dasturiy vosita xavfsizligining fundamental prinsiplari

Dasturiy ta’minot yaratilganida va foydalanilganida qator prinsiplarga amal qilish talab qilinadi. Quyida OWASP tashkiloti tomonidan taqdim etilgan prinsiplar keltirilgan:

Hujumga uchrashi mumkin bo‘lgan soha maydonini minimallashtirish. Dasturiy ta’minotga qo‘shilgan har bir xususiyat dasturga ma’lum miqdordagi xavf darajasini ham qo‘shadi. Dasturni xavfsiz amalga oshirishning maqsadi – hujumga uchrashi mumkin bo‘lgan sohani toraytirish orqali umumiy dasturdagi xavfni kamaytirish. Masalan, web saytlarda onlayn yordamini amalga oshirish uchun qidirish funksiyasi mavjud. Biroq, ushbu imkoniyat web saytga SQL – inyeksiya hujumi bo‘lishi ehtimolini keltirib chiqarishi mumkin. Qidiruv imkoniyati autentifikatsiyadan o‘tgan foydalanuvchilar uchun bo‘lsa, hujum bo‘lishi ehtimoli kamayadi. Agar qidiruv ma’lumotlari markazlashgan tarzda tekshirilsa, ushbu hujum ehtimoli yanada kamayadi.

Xavfsiz standart sozlanmalarini o‘rnatish. Amalda, aksariyat dasturiy ta’minotlarda va operatsion tizimlarda ko‘plab xavfsizlik sozlanmalari standart tartibda o‘rnatilgan bo‘ladi. Biroq, bu foydalanuvchilar tomonidan yaxshi qabul qilinmaydi va shuning uchun, aksariyat hollarda, ushbu sozlanmalarni o‘chirib qo‘yish amalga oshiriladi. Masalan, operatsion tizimlarda parollarni eskirish vaqti standart holda o‘rnatilgan bo‘lsada, aksariyat foydalanuvchilar tomonidan ushbu sozlanma o‘chirib qo‘yiladi.

Minimal imtiyozlar prinsipi. Axborot xavfsizligi, informatika, dasturlash va boshqa sohalarda keng qo‘llaniluvchi minimal imtiyozlar prinsipi (Principle of least privilege) – hisoblash muhitidagi u yoki bu abstraksiya darajasida resurslarga murojaatni tashkil qilish. Bunga ko‘ra har bir modul o‘z vazifasini to‘laqonli bajarishi uchun zarur bo‘lgan resurs yoki axborotdan minimal darajada foydalanish talab etiladi.

Bu prinsip foydalanuvchi yoki dasturchiga faqat o‘z vazifasi uchun zarur bo‘lgan imtiyozlarga ega bo‘lishi kerakligini anglatadi. Masalan, vaqt o‘tkazish uchun ishlab chiqilgan turli mobil o‘yin dasturlari SMS xabarni o‘qish yoki qo‘ng‘iroq qiluvchilar ro‘yxatini bilish imkoniyatiga ega bo‘lishi shart emas. Masalan, dasturlash tillarida (Java dasturlash tilida keltirilgan) obyektlardan foydanishni cheklash uchun turli kalit so‘zlardan foydalaniladi (4.2-jadval).

4.2-jadval

Java dasturlash tilidagi foydalanuvchi imtiyozlari

Imtiyoz / Xususiyat	**Default**	**Private**	**Protected**	**Public**
Bir xil klass	+	+	+	+
Bir paket qismklassi	+	-	+	+
Bir paket qismklassi bo‘lmagan	+	-	+	+
Turli paket qismklasslari	-	-	+	+
Turli paket qismklassi bo‘lmagan	-	-	-	+

Teran himoya prinsipi. Ushbu prinsipga binoan, bitta nazoratning bo‘lishi yaxshi, ko‘plab nazoratlardan foydalanish esa yaxshiroq deb qaraladi. Teran himoyada foydalanilgan nazoratlar turli zaiflik orqali bo‘lishi mumkin bo‘lgan tahdidlarni oldini oladi. Xavfsiz dastur yozish orqali esa, foydalanish qiymatini tekshirish, markazlashgan auditni boshqarish va foydaluvchilarning barcha sahifalardan foydalanishlari ta’minlanishi mumkin.

Agar to‘g‘ri ishlab chiqilgan ma’mur interfeysi, tarmoqdan foydalanish qoidalarini to‘g‘ri bajarsa, foydalanuvchilarning avtorizatsiyasini tekshirsa va barcha holatlarni qaydlasa, u anonim hujumga bardoshsiz bo‘lishi mumkin emas.

Xavfsizlikning buzilishi. Ilovalar, amalga oshirilishi jarayonida turli sabablarga ko‘ra, buzilishlarga uchraydi. Masalan, quyida e’tiborsizlik oqibatida qoldirilgan xavfsizlik holati keltirilgan.

```
isAdmin = true;
try {
  codeWhichMayFail();
  isAdmin = isUserInRole( “Administrator” );
}
catch (Exception ex) {
  log.write(ex.toString());
}
```

Mazkur holda `codeWhichMayFail()` yoki `isUserInRole()` funksiyalarida xatolik bo‘lsa yoki biror `Exception` kuzatilgan taqdirda ham foydalanuvchi ma’mur rolida qolaveradi. Bu ko‘rinib turgan xavfsizlik riski hisoblanadi.

Xizmatlarga ishonmaslik. Hozirgi kunda ko‘plab tashkilotlar uchinchi tomon, sheriklarining hisoblash imkoniyatidan foydalanadi. Masalan, bir tashkilot o‘z ma’lumotlarini o‘z sherigiga tegishli dasturiy ta’minot bilan ishlashi mumkin. Bu holda ularga ishonish kafolatlanmaydi. Masalan, Payme yoki shunga o‘xshash ilovalar bir necha bank kartalaridagi ma’lumotlarni taqdim qiladi. Mazkur holda, har bir bank foydalanuvchi tomonida o‘z ma’lumotlarining to‘g‘ri akslantirilganini tekshirishi lozim.

Vazifalarni ajratish. Firibgarlikni oldini olishga qaratilgan asosiy chora – vazifalarni ajratish. Masalan, tashkilotda kompyuter olish bo‘yicha talab yuborgan odam tomonidan uni qabul qilinmasligi shart. Sababi, bu holda u ko‘plab kompyuterlarni so‘rashi va qabul qilib olganini rad qilishi mumkin. Ba’zi holda, bir rol uchun oddiy foydalanuvchilarga nisbatan ishonch darajasi turlicha bo‘ladi. Masalan, ma’murlar tizimni o‘chirishi yoki yoqishi, parollar siyosatini o‘rnata olishi kerak. Biroq, ular onlayn savdo do‘koniga imtiyozga ega foydalanuvchi sifatida kira olmasligi, xususan, tovarlarni boshqalar nomidan sotib olish imkoniyatiga ega bo‘lmasligi kerak.

Xavfsizlikni noaniqlikdan saqlash. Noaniqlikka asoslangan xavfsiz – zaif xavfsizlik bo‘lib, birinchi nazoratning o‘zida xatolikka uchraydi. Bu biror sirni saqlash yomon g‘oya ekanligini anglatmasada, xavfsizlikning muhim jihatlari tafsilotlarining yashirin bo‘lishiga asoslanmasligini bildiradi.

Masalan, dastur xavfsizligi uning ochiq kodidan xabardor bo‘linganida barbod bo‘lmasligi kerak. Xavfsizlik ko‘plab boshqa omillarga, masalan, parolning oqilona siyosatiga, tarmoq arxitekturasiga, auditni boshqarish vositalariga tayanishi lozim.

Bunga amaliy misol sifatida, Linux operatsion tizimini keltirish mumkin. Ushbu operatsion tizimning kodi ochiq hisoblansada, to‘g‘ri himoyalangan va shuning uchun, hozirgi kundagi mustahkam operatsion tizimlardan biri hisoblanadi.

Xavfsizlikni soddaligi. Hujumga uchrash soha maydoni va soddalik bir-biriga bog‘liq. Ba’zi dasturiy ta’minot muhandislari kodning sodda ko‘rinishidan ko‘ra murakkabligini afzal ko‘radilar. Biroq, sodda va tushunishga oson ko‘rinish tezkor bo‘lishi mumkin. Shuning uchun, dasturiy ta’minotni yaratish jarayonida murakkablikdan qochishgaharakat qilish zarur.

Dasturiy mahsulotlarga qo‘yilgan xavfsizlik talablari. Dasturiy ta’minotni ishlab chiqishda unga ko‘plab talablar qo‘yiladi.

Dasturiy mahsulotlarga qo‘yiladigan talablar uch turga bo‘linadi:

- vazifaviy talablar:
    - tizim amalga oshirilishida kerak bo‘lgan vazifalar.
- novazifaviy talablar:
    - tizimning xususiyatlariga qo‘yilgan talablar.

Vazifaviy talablar. Bu talablar quyidagilarni o‘z ichiga oladi:

- tizim kutgan kirishga qo‘yilgan talablar;
- tizimdan chiqqan natijaga qo‘yilgan talablar;
- kirish va chiqishga aloqador bo‘lgan talablar.

Novazifaviy talablar. Novazifaviy talablarga quyidagilar taalluqli:

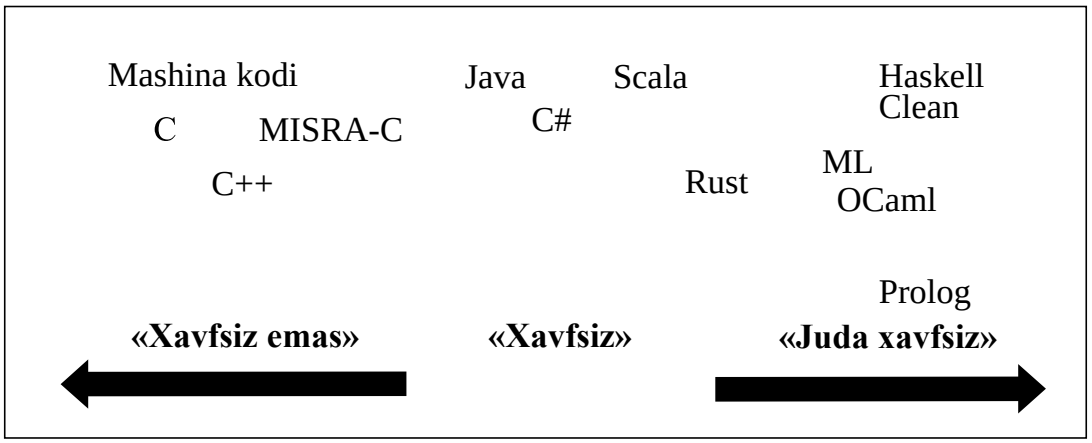
- audit qilish imkoniyati;
- kengaytirish mumkinligi;
- foydalanishga qulayligi;
- bajarilishi;
- ixchamligi;
- ishonchliligi;
- xavfsizligi;
- testlash imkoniyati;

- foydalanuvchanligi va h.

Xususiy xavfsizlik talablariga quyidagilar taalluqli:

– maxfiylik talabiga misol:
  - tizim ruxsat berilgan foydalanuvchigagina .doc fayllarni ko‘rsatishi kerak;
  - xavfsiz aloqa kanalidan foydalanish.
– ruxsatlarni nazoratlash talabiga misol:
  - tizim paroldan foydalanishni talab etishi kerak;
  - rollarga asoslangan foydalanishga ruxsatlarni nazoratlash amalga oshirilishi kerak.
– butunlik talabiga misol:
  - ochiq (public) turdagi foydalanuvchilar uchun faqat o‘qish, maxfiy (private) turidagi foydalanuvchilar uchun ham o‘qish ham yozish huquqi berilishi.
– foydalanuvchanlik talabiga misol:
  - barcha qayd yozuvlarda parol bo‘lishi shart;
  - 3 ta muvaffaqqiyatsiz urinishdan so‘ng qayd yozuvi blokirovkalanishi shart;
  - qayd yozuviga 5 min davomida tahdid amalga oshirilmasa u blokirovkadan yechilishi shart.

Dasturlash tiliga asoslangan xavfsizlik. Turli dasturlash tillari o‘ziga xos imkoniyatlarga ega, dasturlash sathida xavfsizlikni ta’minlash muhim ahamiyat kasb etadi. Mavjud dasturlash tillarini xavfsiz yoki xavfsiz emas turlariga ajratish nisbiy tushuncha bo‘lib, ularni quyidagicha tasvirlash mumkin (7.5-rasm).



4.5– rasm. Dasturlash tillarining xavfsizlik darajasining sodda ko‘rinishi

4.3.Kompyuter viruslari va virusdan himoyalanish muammolari

Kompyuter virusining ko‘p ta’riflari mavjud. Birinchi ta’rifni 1984 yili Fred Koen bergan: “Kompyuter virusi – boshqa dasturlarni, ularga o‘zini yoki o‘zgartirilgan nusxasini kiritish orqali, ularni modifikatsiyalash bilan zaharlovchi dastur. Bunda kiritilgan dastur keyingi ko‘payish qobiliyatini saqlaydi”. Virusning o‘z-o‘zidan ko‘payishi va hisoblash jarayonini modifikatsiyalash qobiliyati bu ta’rifdagi tayanch tushunchalar hisoblanadi. Kompyuter virusining ushbu xususiyatlari tirik tabiat organizmlarida biologik viruslarning parazitlanishiga o‘hshash.

Hozirda kompyuter virusi deganda quyidagi xususiyatlarga ega bo‘lgan dasturiy kod tushuniladi:

– asliga mos kelishi shart bo‘lmagan, ammo aslining xususiyatlariga (o‘z-o‘zini tiklash) ega bo‘lgan nusxalarni yaratish qobiliyati;

– hisoblash tizimining bajariluvchi obyektlariga yaratiluvchi nusxalarning kiritilishini ta’minlovchi mexanizmlarning mavjudligi.

Ta’kidlash lozimki, bu xususiyatlar zaruriy, ammo yetarli emas. Ko‘rsatilgan xususiyatlarni hisoblash muhitidagi zarar keltiruvchi dastur ta’sirining destruktivlik va sir boy bermaslik xususiyatlari bilan to‘ldirish lozim.

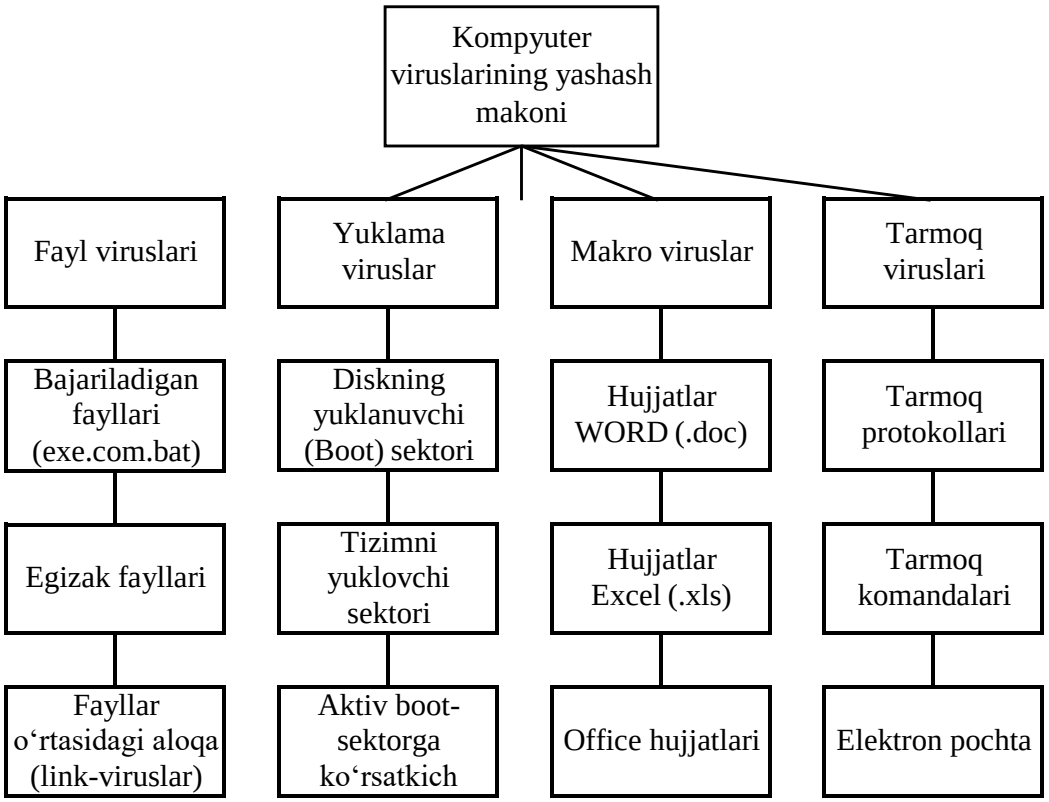
Viruslarni quyidagi asosiy alomatlari bo‘yicha turkumlash mumkin:

– yashash makoni;
– operatsion tizim;
– ishlash algoritmi xususiyati;
– destruktiv imkoniyatlari.

Kompyuter viruslarini yashash makoni, boshqacha aytganda viruslar kiritiluvchi kompyuter tizimi obyektlarining xili bo‘yicha turkumlash keng tarqalgan (7.6-rasm).

Fayl viruslari bajariluvchi fayllarga turli usullar bilan kiritiladi (eng ko‘p tarqalgan viruslar xili), yoki fayl-egizaklarni (kompanon viruslar) yaratadi yoki faylli tizimlarni (link-viruslar) tashkil etish xususiyatidan foydalanadi.

Yuklama viruslar o‘zini diskning yuklama sektoriga (boot - sektoriga) yoki vinchesterning tizimli yuklovchisi (MasterBootRecord) bo‘lgan sektorga yozadi. Yuklama viruslar tizim yuklanishida boshqarishni oluvchi dastur kodi vazifasini bajaradi.



4.6-rasm. Yashash makoni bo‘yicha kompyuter viruslarining turkumlanishi

Makroviruslar axborotni ishlovchi zamonaviy tizimlarning makrodasturlarini va fayllarini, xususan Microsoft Word, Microsoft Excel va h. kabi ommaviy muharrirlarning fayl-hujjatlarini va elektronjadvallarini zaharlaydi.

Tarmoq viruslari o‘zini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi. Ba’zida tarmoq viruslarini “qurt” xilidagi dasturlar deb yuritishadi. Tarmoq viruslari Internet-qurtlarga (Internet bo‘yicha tarqaladi), IRC-qurtlarga (chatlar, InternetRelayChat) bo‘linadi.

Kompyuter viruslarining ko‘pgina kombinasiyalangan xillari ham mavjud, masalan – tarmoqli makrovirus tahrirlanuvchi hujjatlarni zaxarlaydi, hamda o‘zining nusxalarini elektron pochta orqali tarqatadi. Boshqa bir misol sifatida fayl-yuklama viruslarini ko‘rsatish mumkinki, ular fayllarni hamda disklarning yuklanadigan sektorini zaharlaydi.

Viruslarning hayot davri.Har qanday dasturdagidek kompyuter viruslari hayot davrining ikkita asosiy bosqichini - saqlanish va bajarilish bosqichlarini ajratish mumkin.

Saqlanish bosqichi virusning diskda u kiritilgan obyekt bilan birgalikda shundaygina saqlanish davriga to‘g‘ri keladi. Bu bosqichda

virus virusga qarshi dastur ta’minotiga zaif bo‘ladi, chunki u faol emas va himoyalanish uchun operatsion tizimni nazorat qila olmaydi.

Kompyuter viruslarining *bajarilish davri*, odatda, beshta bosqichni o‘z ichiga oladi:

1. Virusni xotiraga yuklash.
2. Qurbonni qidirish.
3. Topilgan qurbonni zaharlash.
4. Destruktiv funksiyalarni bajarish.
5. Boshqarishni virus dastur-eltuvchisiga o‘tkazish.

Virusni xotiraga yuklash. Virusni xotiraga yuklash operatsion tizim yordamida virus kiritilgan bajariluvchi obyekt bilan bir vaqtda amalga oshiriladi. Masalan, agar foydalanuvchi virus bo‘lgan dasturiy faylniishga tushirsa, ravshanki, virus kodi ushbu fayl qismi sifatida xotiraga yuklanadi. Oddiy holda, virusni yuklash jarayoni-diskdan operativ xotiraga nusxalash bo‘lib, so‘ngra boshqarish virus badani kodiga uzatiladi. Bu harakatlar operatsion tizim tomonidan bajariladi, virusning o‘zi passiv holatda bo‘ladi. Murakkabroq vazifalarda virus boshqarishni olganidan so‘ng o‘zining ishlashi uchun qo‘shimcha harakatlarni bajarishi mumkin. Bu bilan bog‘liq ikkita jihat ko‘riladi.

Birinchisi viruslarni aniqlash muolajasining maksimal murakkablashishi bilan bog‘liq. Saqlanish bosqichida ba’zi viruslar himoyalanishni ta’minlash maqsadida yetarlicha murakkab algoritmdan foydalanadi. Bunday murakkablashishga virus asosiy qismini shifrlashni kiritish mumkin. Ammo faqat shifrlashni ishlatish chala chora hisoblanadi, chunki yuklanish bosqichida rasshifrovkani ta’minlovchi virus qismi ochiq ko‘rinishda saqlanishi lozim. Bunday holatdan qutilish uchun viruslarni ishlab chiquvchilar rasshifrovka qiluvchi kodni “mutatsiyalash” mexanizmidan foydalanadi. Bu usulning mohiyati shundan iboratki, obyektga virus nusxasi kiritilishida uning rasshifrovka qilinishiga taalluqli qismi shunday modifikatsiyalanadiki, original bilan matnli farqlanish paydo bo‘ladi, ammo ish natijasi o‘zgarmaydi.

Kodni mutatsiyalash mexanizmidan foydalanuvchi viruslar *polimorf viruslar* nomini olgan. Polimorf viruslar (polymorphic)-qiyin aniqlanadigan viruslar bo‘lib, signaturalarga ega emas, ya’ni tarkibida birorta ham kodining doimiy qismi yo‘q. Polimorfizm faylli, yuklamali va makroviruslarda uchraydi.

Stels-algoritmlardan foydalanilganda viruslar o‘zlarini tizimda to‘la yoki qisman bekitishlari mumkin. stels-algoritmlaridan foydalanadigan viruslar – *stels-viruslar* (Stealth) deb yuritiladi. Stels viruslar operatsion

tizimning shikastlangan fayllarga murojaatini ushlab qolish yo‘li bilan o‘zini yashash makonidaligini yashiradi va operatsion tizimni axborotni shikastlanmagan qismiga yo‘naltiradi.

Ikkinchi jihat *rezident viruslar* deb ataluvchi viruslar bilan bog‘liq. Virus va u kiritilgan obyekt operatsion tizim uchun bir butun bo‘lganligi sababli, yuklanishdan so‘ng ular, tabiiy, yagona adres makonida joylashadi. Obyekt ishi tugaganidan so‘ng u operativ xotiradan bo‘shaladi. Bunda bir vaqtning o‘zida virus ham bo‘shalib saqlanishning passiv bosqichiga o‘tadi. Ammo ba’zi viruslar xili xotirada saqlanish va virus eltuvchi ishi tugashidan so‘ng faol qolish qobiliyatiga ega. Bunday viruslar rezident nomini olgan. Rezident viruslar, odatda, faqat operatsion tizimga ruxsat etilgan imtiyozli rejimlardan foydalanib yashash makonini zaharlaydi va ma’lum sharoitlarda zararkunandalik vazifasini bajaradi. Rezident viruslar xotirada joylashadi va kompyuter o‘chirilishigacha yoki operatsion tizim qayta yuklanishigacha faol holda bo‘ladi.

Rezident bo‘lmagan viruslar faqat faollashgan vaqtlarida xotiraga tushib zaharlash va zarakunandalik vazifalarini bajaradi. Keyin bu viruslar xotirani butunlay tark etib yashash makonida qoladi.

Ta’kidlash lozimki, viruslarni rezident va rezident bo‘lmaganlarga ajratish faqat fayl viruslariga taalluqli. Yuklanuchi va makroviruslar rezident viruslarga tegishli.

Qurbonni qidirish. Qurbonni qidirish usuli bo‘yicha viruslar ikkita sinfga bo‘linadi. Birinchi sinfga operatsion tizim funksiyalaridan foydalanib faol qidirishni amalga oshiruvchi viruslar kiradi. Ikkinchi sinfga qidirishning passiv mexanizmlarini amalga oshiruvchi, ya’ni dasturiy fayllarga tuzoq qo‘yuvchi viruslar taalluqli.

Topilgan qurbonni zaharlash. Oddiy holda zaharlash deganda qurbon sifatida tanlangan obyektda virus kodining o‘z-o‘zini nusxalashi tushuniladi.

Avval fayl viruslarining zaharlash xususiyatlarini ko‘raylik. Bunda ikkita sinf viruslari farqlanadi. Birinchi sinf viruslari o‘zining kodini dasturiy faylga bevosita kiritmaydi, balki fayl nomini o‘zgartirib, virus badani bo‘lgan yangi faylni yaratadi. Ikkinchi sinfga qurbon fayllariga bevosita kiruvchi viruslar taalluqli. Bu viruslar kiritilish joylari bilan xarakterlanadi. Quyidagi variantlar bo‘lishi mumkin:

1. Fayl boshiga kiritish. Ushbu usul MS-DOSning *com*-fayllari uchun eng qulay hisoblanadi, chunki ushbu formatda xizmatchi sarlavhalar ko‘zda tutilgan.

2. Fayl oxiriga kiritish. Bu usul eng ko‘p tarqalgan bo‘lib, viruslar

kodiga boshqarishni uzatish dasturning birinchi komandasi (*com*) yoki fayl sarlavhasini (*exe*) modifikatsiyalash orqali ta’minlanadi.

3. Fayl o‘rtasiga kiritish. Odatda bu usuldan viruslar strukturasi oldindan ma’lum fayllarga (masalan, *Command.com* fayli) yoki tarkibida bir xil qiymatli baytlar ketma-ketligi bo‘lgan, uzunligi virus joylashishiga yetarli fayllarga tatbiqan foydalaniladi.

Yuklama viruslar uchun zaharlash bosqichining xususiyatlari ular kiritiluvchi obyektlar – qayishqoq va qattiq disklarning yuklanish sektorlarining sifati va qattiq diskning bosh yuklama yozuvi (MBR) orqali aniqlanadi. Asosiy muammo-ushbu obyekt o‘lchamlarining chegaralanganligi. Shu sababli, viruslar o‘zlarining qurbon joyida sig‘magan qismini diskda saqlashi, hamda zaharlangan yuklovchi original kodini tashishi lozim.

Makroviruslar uchun zaharlash jarayoni tanlangan hujjat-qurbonda virus kodini saqlashdan iborat. Ba’zi axborotni ishlash dasturlari uchun buni amalga oshirish oson emas, chunki hujjat fayllari formatining makroprogrammalarni saqlashi ko‘zda tutilmagan bo‘lishi mumkin.

Destruktiv funksiyalarni bajarish. Destruktiv imkoniyatlari bo‘yicha beziyon, xavfsiz, xavfli va juda xavfli viruslar farqlanadi.

Beziyon viruslar - o‘z-o‘zidan tarqalish mexanizmi amalga oshiriluvchi viruslar. Ular tizimga zarar keltirmaydi, faqat diskdagi bo‘sh xotirani sarflaydi xolos.

Xavfsiz viruslar – tizimda mavjudligi turli taassurot (ovoz, video) bilan bog‘liq viruslar, bo‘sh xotirani kamaytirsada, dastur va ma’lumotlarga ziyon yetkazmaydi.

Xavfli viruslar – kompyuter ishlashida jiddiy nuqsonlarga sabab bo‘luvchi viruslar. Natijada dastur va ma’lumotlar buzilishi mumkin.

Juda xavfli viruslar – dastur va ma’lumotlarni buzilishiga hamda kompyuter ishlashiga zarur axborotni o‘chirilishiga bevosita olib keluvchi, muolajalari oldindan ishlash algoritmlariga joylangan viruslar.

Boshqarishni virus dastur – eltuvchisiga o‘tkazish. Ta’kidlash lozimki, viruslar buzuvchilar va buzmaydiganlarga bo‘linadi.

Buzuvchi viruslar dasturlar zaharlanganida ularning ishga layoqatligini saqlash xususida qayg‘urmaydilar, shu sababli ularga ushbu bosqichning ma’nosi yo‘q.

Buzmaydigan viruslar uchun ushbu bosqich xotirada dasturni korrekt ishlanishi shart bo‘lgan ko‘rinishda tiklash va boshqarishni virus dastur-eltuvchisiga o‘tqazish bilan bog‘liq.

Zarar keltiruvchi dasturlarning boshqa xillari. Viruslardan tashqari zarar keltiruvchi dasturlarning quyidagi xillari mavjud:

– troyan dasturlari;

– mantiqiy bombalar;

– masofadagi kompyuterlarni yashirincha ma’murlovchi xaker utilitalari;

– Internetdan va boshqa konfidensial axborotdan foydalanish parollarini o‘g‘rilovchi dasturlar.

Ular orasida aniq chegara yo‘q: troyan dasturlari tarkibida viruslar bo‘lishi, viruslarga mantiqiy bombalar joylashtirilishi mumkin va h.

Troyan dasturlar o‘zlari ko‘paymaydi va tarqatilmaydi. Tashqaridan troyan dasturlar mutlaqo beozor ko‘rinadi, hatto foydali funksiyalarni tavsiya etadi. ammo foydalanuvchi bunday dasturni kompyuteriga yuklab, ishga tushirsa, dastur bildirmay zarar keltiruvchi funksiyalarni bajarishi mumkin. Ko‘pincha troyan dasturlar viruslarni dastlabki tarqatishda, Internet orqali masofadagi kompyuterdan foydalanishda, ma’lumotlarni o‘g‘rilashda yoki ularni yo‘q qilishda ishlatiladi.

Mantiqiy bomba – ma’lum sharoitlarda zarar keltiruvchiharakatlarni bajaruvchi dastur yoki uning alohida modullari. Mantiqiy bomba, masalan, ma’lum sana kelganida yoki ma’lumotlar bazasida yozuv paydo bo‘lganida yoki yo‘q bo‘lganida va h. ishga tushishi mumkin. Bunday bomba viruslarga, troyan dasturlarga va oddiydasturlarga joylashtirilishi mumkin.

Viruslar va zarar keltiruvchi dasturlarni tarqatish kanallari. Kompyuterlar va korporativ tarmoqlarni himoyalovchi samarador tizimni yaratish uchun qayerdan xavf tug‘ilishini aniq tasavvur etish lozim. Viruslar tarqalishning juda xilma-xil kanallarini topadi. Buning ustiga eski usullarga yangisi qo‘shiladi.

Tarqatishning klassik (mumtoz) usullari. Fayl viruslari dastur fayllari bilan birgalikda disketlar va dasturlar almashishda, tarmoq kataloglaridan, Web- yoki FTP – serverlardan dasturlar yuklanishida tarqatiladi. Yuklama viruslar kompyuterga foydalanuvchi zaharlangan disketani diskovodda qoldirib, so‘ngra operatsion tizimni qayta yuklashida tushib qoladi. Yuklama virus kompyuterga viruslarning boshqa xili orqali kiritilishi mumkin. Makrokomanda viruslari Microsoft Word, Excel, Access fayllari kabi ofis hujjatlarining zaxarlangan fayllari almashinishida tarqaladi.

Agar zaharlangan kompyuter lokal tarmoqqa ulangan bo‘lsa virus

osongina fayl-server disklariga tushib qolishi, u yerdan kataloglar orqali tarmoqning barcha kompyuterlariga o‘tishi mumkin. Shu tariqa virus epidemiyasi boshlanadi. Virus tarmoqda shu virus tushib qolgan kompyuter foydalanuvchisi xuquqlari kabi xuquqqa ega ekanligini tizim ma’muri unutmasligi lozim. Shuning uchun u foydalanuvchi foydalanadigan barcha kataloglarga tushib qolishi mumkin. Agar virus tarmoq ma’muri ishchi stansiyasiga tushib qolsa oqibati juda og‘ir bo‘lishi mumkin.

Elektron pochta. Hozirda Internet global tarmog‘i viruslarning asosiy manbai hisoblanadi. Viruslar bilan zaharlanishlarning aksariyati MicroSoftWord formatida xatlar almashishda sodir bo‘ladi. Elektron pochta makroviruslarni tarqatish kanali vazifasini o‘taydi, chunki axborot bilan bir qatorda ko‘pincha ofis hujjatlari jo‘natiladi.

Viruslar bilan zaharlash bilmasdan va yomon niyatda amalga oshirilishi mumkin. Masalan, makrovirus bilan zaharlangan muharrirdan foydalanuvchi o‘zi shubha qilmagan holda, adresatlarga zaharlangan xatlarni jo‘natishi mumkin. Ikkinchi tarafdan niyatibuzuq atayin elektron pochta orqali harqanday xavfli dasturiy kodni jo‘natishi mumkin.

Troyan Web-saytlar. Foydalanuvchilar virusni yoki troyan dasturni Internet saytlarining oddiy kuzatishda, troyan Web-saytni ko‘rganida olishi mumkin. Foydalanuvchi brauzerlaridagi xatoliklar ko‘pincha troyan Web-saytlari faol komponentlarining foydalanuvchi kompyuterlariga zarar keltiruvchi dasturlarni kiritishiga sabab bo‘ladi. Troyan saytni ko‘rishga taklifni foydalanuvchi oddiy elektron xat orqali olishi mumkin.

Lokal tarmoqlar. Lokal tarmoqlar ham tezlikda zaharlanish vositasi hisoblanadi. Agar himoyaning zaruriy choralari ko‘rilmasa, zaharlangan ishchi stansiya lokal tarmoqqa kirishda serverdagi bir yoki bir necha xizmatchi fayllarni zaharlaydi. Bunday fayllar sifatida Login.com xizmatchi faylni, firmada qo‘llaniluvchi Excel-jadvallar va standart hujjat-shablonlarni ko‘rsatish mumkin. Foydalanuvchilar bu tarmoqqa kirishida serverdan zaharlangan fayllarni ishga tushiradi, natijada virus foydalanuvchi kompyuteridan foydalana oladi.

Zarar keltiruvchi dasturlarni tarqatishning boshqa kanallari. Viruslarni tarqatish kanallaridan biri dasturiy ta’minotning qaroqchi nusxalari hisoblanadi. Disketlar va CD-disklardagi noqununiy nusxalarda ko‘pincha turli-tuman viruslar bilan zaharlangan fayllar bo‘ladi. Viruslarni tarqatish manbalariga elektron anjumanlar va FTP va BBS fayl-serverlar ham taalluqli.

O‘quv uslubiy yurtlarida va Internet-markazlarida o‘rnatilgan va umumfoydalanish rejimida ishlovchi kompyuterlar ham osongina viruslarni tarqatish manbaiga aylanishi mumkin. Agar bunday kompyuterlardan biri navbatdagi foydalanuvchi disketidan zaharlangan bo‘lsa, shu kompyuterda ishlovchi boshqa foydalanuvchilar disketlari ham zaharlanadi.

Kompyuter texnologiyasining rivojlanishi bilan kompyuter viruslari ham, o‘zining yangi yashash makoniga moslashgan holda, takomillashadi. Har qanday onda yangi, oldin ma’lum bo‘lmagan yoki ma’lum bo‘lgan, ammo yangi kompyuter asbob-uskunasiga mo‘ljallangan kompyuter viruslari, troyan dasturlari va qurtlar paydo bo‘lishi mumkin. Yangi viruslar ma’lum bo‘lmagan yoki oldin mavjud bo‘lmagan tarqatish kanallaridan hamda kompyuter tizimlarga tatbiq etishning yangi texnologiyalaridan foydalanishi mumkin. Virusdan zaharlanish xavfini yo‘qotish uchun korporativ tarmoqning tizim ma’muri, nafaqat virusga qarshi usullardan foydalanishi, balki kompyuter viruslari dunyosini doimo kuzatib borishi shart.

Zararli dasturiy vositalarni aniqlash. Zararli dasturiy vositalarni aniqlashda asosan uchta yondashuvdan foydalaniladi. Birinchisi va eng keng tarqalgani *signaturaga asoslangan aniqlash* bo‘lib, zararli dasturdagi shablon yoki signaturani topishga asoslanadi. Ikkinchi yondashuv *o‘zgarishlarni aniqlashga* asoslangan bo‘lib, o‘zgarishga uchragan fayllarni aniqlaydi. O‘zgarishi kutilmagan fayl o‘zgarganida zararlangan deb topiladi. Uchinchi yondashuv *anomaliyaga asoslangan*, noodatiy yoki virusga o‘xshash fayllarni va holatlarni aniqlashga asoslanadi.

Signaturaga asoslangan aniqlash. Signatura bu – faylda topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin. Biroq, bu usul kam moslashuvchanlik darajasiga ega bo‘lib, virus yozuvchilari tomonidan osongina chetlanib o‘tilishi mumkin.

Masalan, W32/Beast virusi (1999 yilda aniqlangan Microsoft Word hujjatini zararlashga qaratilgan virus) uchun 83EB 0274 EBOE 740A 81EB 0301 0000 signaturasi foydalanilgan. Bu holda tizimdagi barcha fayllar ichida ushbu signatura qidiriladi. Biroq, biror fayl ichida ushbu signatura aniqlangan vaqtda ham to‘liq virusni topdik deb aytish mumkin emas. Sababi, biror virus bo‘lmagan fayl tarkibida ham ushbu signatura bo‘lishi mumkin. Agar qidiriladigan fayllarda bitlar tasodifiy bo‘lsa, ushbu holatning bo‘lishi ehtimoli $1/2^{112}$ ga teng bo‘ladi. Biroq, kompyuter

dasturlari va ma’lumotlar ichidagi bitlar tasodifiylikdan yiroq va bu ehtimolni yanada ortishini anglatadi. Boshqacha aytganda, biror fayldan signatura aniqlangan taqdirda ham, uni qo‘shimcha tekshirish amalga oshirilishi zarur.

Signaturaga asoslangan aniqlash usuli virus aniq bo‘lganida va umumiy bo‘lgan signaturalar ajratilgan holatda juda yuqori samaradorlikka ega. Bundan tashqari, ushbu usulga binoan foydalanuvchi va ma’murga minimal yuklama yuklanadi va ularga faqat signaturalarni saqlash va uzluksiz yangilash vazifasi qo‘yiladi.

Biroq, signaturalar saqlangan faylning hajmi katta bo‘lib, 10 yoki 100 minglab signaturaga ega fayl yordamida skanerlash juda ko‘p vaqt oladi. Bundan tashqari, biror aniqlangan virusni kichik o‘zgartirish orqali ushbu usulni osonlik bilan aldab o‘tish mumkin.

Hozirgi kunda signaturaga asoslangan tanib olish usuli zamonaviy antivirus yoki zararli dasturlarga qarshi himoya vositalarida keng qo‘llaniladi.

O‘zgarishlarni aniqlovchi usul. Zararli dasturlar ma’lum manzilda joylashganligi sababli, tizimdagi biror joyda o‘zgarish aniqlansa, zararlangan joyini ko‘rsatish mumkin. Ya’ni, agar o‘zgarishga uchragan fayl aniqlansa, u virus orqali zararlangan bo‘lishi mumkin.

O‘zgarishlarni qanday aniqlash mumkin? Ushbu muammoni yechishda xesh-funksiyalar mos keladi. Faraz qilaylik, tizimdagi barcha fayllar xeshlanib, xesh qiymatlari xavfsiz manzilda saqlangan bo‘lsin. U holda vaqti-vaqti bilan ushbu faylning xesh qiymatlari qaytadan hisoblanadi va dastlabkilari bilan taqqoslanadi. Agar faylning bir yoki bir nechta bitlari o‘zgarishga uchragan bo‘lsa, xesh qiymatlar bir biriga mos kelmaydi va fayl virus tomonidan zararlangan hisoblanadi.

Ushbu usulning afzalliklaridan biri shuki, agar fayl zararlangan bo‘lsa, uni to‘liq aniqlash mumkin. Bundan tashqari, oldin noma’lum bo‘lgan zararli dasturni ham aniqlash mumkin.

Biroq, ushbu usul kamchiliklarga ham ega. Tizimdagi fayllar odatda tez-tez o‘zgarib turadi va natijada yolg‘ondan zararlangan deb topilgan holatlar soni ortadi. Agar virus tizimdagi tez-tez o‘zgaruvchi fayl ichiga joylashtirilgan bo‘lsa, ushbu usulni osonlik bilan aylanib o‘tish mumkin. Bu holda ushbu fayldagi o‘zgarishni log fayl orqali aniqlash ko‘p vaqt talab qiladi va bu signaturaga asoslangan usuldagi kabi muammolarga olib keladi.

Anomaliyaga asoslangan aniqlash. Anomaliyaga asoslangan usul noodatiy yoki virusga o‘xshash yoki bo‘lishi mumkin bo‘lgan zararli

harakatlarni yoki xususiyatlarni topishni maqsad qiladi. Ushbu g‘oya IDS tizimlarida ham foydalaniladi.

Ushbu usulning fundamental muammosi - qaysi holatni normal va qaysi holatni normal bo‘lmagan deb topish hamda ushbu ikki holat orasidagi farqni aniqlash hisoblanadi. Bundan tashqari, normal holatning o‘zgarishi va tizimning bu holatga moslashish muammosi ham mavjud. Bu esa ko‘plab noto‘g‘ri signallarni paydo bo‘lishiga sabab bo‘ladi.Ushbu usulning afzalligi sifatida oldin noma’lum bo‘lgan zararli dasturlarni aniqlash imkonini ko‘rsatish mumkin.

Antivirus dasturiy vositalarining kamchiligi. Antivirus dasturiy vositasiga kompyuterni himoyalashda amalga oshirilish lozim bo‘lgan zaruriy shart sifatida qaraladi. Umuman olganda, antivirus kompyuter uchun zararli dasturlarni skanerlashni, himoyalashni, karantin holatiga tushirishni va boshqa amallarni bajaradi. Antivirus dasturiy vositalarini CD-disklardan va Internet tarmog‘idan foydalangan holda o‘rnatish mumkin. Antivirus dasturiy vositalari bir biridan ko‘plab o‘ziga xos xususiyatlari bilan ajralib turadi. Masalan, Internet tarmog‘idan foydalanilganda reklamalarni blokirovkalash, Internet tarmog‘idan kirib keluvchi zararli dasturlarni blokirovkalash va h. Biroq, foydalanuvchilar to‘liq antivirus dasturiy vositalarining imkoniyatilariga ishonib qolmasliklari lozim.

Viruslarni doimiy aniqlash uchun antivirus dasturiy vositalari eng yangi va yangilangan ma’lumotlarni o‘z ichiga olgan namunaviy fayllarga muxtoj. Biroq, antivirus ishlab chiqaruvchilari yangi virus uchun namunaviy fayllar yaratgunlaricha virus ishlab chiqaruvchilari tomonidan katta hajmdagi yangi viruslar yaratiladi. Bu esa, yangi virus uchun vaksinani tayyorlash yetarlicha ko‘p vaqtni talab qiladi.

Bundan tashqari, antivirus dasturi Rootkit tipidagi zararli dasturlarni aniqlashda foydasi tegmasligi mumkin. Rootkit tipidagi zararli dasturlar kompyuter operatsion tizimining markaziga hujum qilishni maqsad qiladi.

Antivirus dasturiy vositalari sifatini baholash omillari. Antivirus dasturiy vositalari quyidagi omillarga ko‘ra baholanishi mumkin:

- *ishonchlik va foydalanishdagi qulaylik* – antivirus dasturiy vositasini “qotib qolishi” va foydalanish uchun turli tayyorganlikni talab etmasligi;
- barcha keng tarqalgan viruslarni sifatli aniqlash, hujjat fayllari/ jadvallari (MS Word, Excel), paketlangan, arxivlangan fayllarni skanerlash va zararlangan obyektlarni davolash qobiliyati;

- barcha mashhur platformalar uchun mavjudligi (DOS, Windows NT, Novell NetWare, OS/2, Alpha, Linux va boshq), talab bo‘yicha va tezkor skanerlash rejimlarining mavjudligi;
- ishlash tezligi va boshqa xususiyatlari.

Antivirus dasturiy komplekslari. Har bir antivirus dasturiy vositalar o‘ziga xos afzallik va kamchiliklarga ega. Faqat bir necha antivirus dasturiy vositalaridan kompleks foydalanish to‘liq himoyani ta’minlashi mumkin. Amalda ko‘plab antivirus dasturiy vositalar mavjud, ularga quyidagilarni misol sifatida keltirish mumkin (7.3-jadval).

4.3-jadval

Turli antivirus dasturlarining xususiyatlari

Mahsulot / Xususiyati	**McAfee AntiVirus Plus**	**Semantec Norton AntiVirus Plus**	**Kaspersky Anti-Virus**	**Bitdefender Antivirus Plus**	**Webroot SecureAnywhere Antivirus**	**Eset Nod32 Antivirus**	**Trend Micro Antivirus+ Security**	**F-secure Anti-Virus**	**VoodooSoft VoodooShield**	**The Kure**
Narxi	19.99$	19.99$	29.99$	29.99$	18.99$	27.99$	29.95$	39.99$	19.99$	19.99$
Talabga ko‘ra skanerlash	+	+	+	+	+	+	+	+	-	-
Doimiy skanerlash	+	+	+	+	+	+	+	+	+	-
Web saytni baholash	+	+	+	-	+	-	+	-	-	-
Zararli URL ni bloklash	+	+	+	+	+	+	+	+	-	-
Fishingdan himoyalash	+	+	+	+	+	+	+	-	-	-
Xususi-yatga ko‘ra aniqlash	+	+	+	+	+	+	+	+	+	-
Zaifliklarni skanerlash	+	-	+	+	-	-	-	-	-	-

Profilaktik choralar. Viruslar va virus yuqtirilgan fayllarni o‘z vaqtida aniqlash, aniqlangan viruslarni har bir kompyuterda to‘liq yo‘q qilish orqali virus epidemiyasining boshqa kompyuterlarga tarqalishini

oldini olish mumkin. Har qanday virusni aniqlaydigan va yo‘q qilinishini kafolatlaydigan mutlaqo ishonchli dasturlar mavjud emas. Kompyuter viruslariga qarshi kurashishning muhim usuli - o‘z vaqtida profilaktika qilishdir. Virusdan zararlanish ehtimolini sezilarli darajada kamaytirish va disklarda ma’lumotlarning ishonchli saqlanishini ta’minlash uchun quyidagi profilaktik choralar ko‘rilishi kerak:

- faqat litsenziyali dasturiy ta’minotdan foydalanish;
- kompyuterni zamonaviy antivirus dasturiy vositasi bilan ta’minlash va uni muntazam yangilab borish;
- boshqa komyuterdan yozib olingan ma’lumotlarni o‘qishdan oldin har bir saqlagichni antivirus tekshiruvidan o‘tkazish;
- arxivlangan fayllarni ajratgandan so‘ng skanerlashni amalga oshirish;
- kompyuter disklarini takroriy antivirus dasturlari tekshiruvidan o‘tkazish;
- kompyuter tarmoqlaridan olingan barcha bajariladigan fayllarni nazoratlashda antivirus dasturidan foydalanish.

Nazorat savollari

1. Dasturiy mahsulotlarda xavfsizlik ta’minlanishining muhimligi.
2. Dasturiy mahsulotlarda xavfsizlik muammolarining kelib chiqish sabablari.
3. Nuqson, bag, xotirani to‘lib toshishi tushunchalari.
4. Dasturiy vosita xavfsizligini fundamental prinsiplari.
5. Dasturiy vositalarga qo‘yilgan talablar.
6. Dasturiy vositalarga qo‘yilgan xavfsizlik talablari.
7. Dasturiy vositalar xavfsizligini ta’minlashda dasturlash tillarining o‘rni.
8. Xavfsiz va xavfsiz bo‘lmagan dasturlash tillari.
9. Zararli dasturlar va ularning asosiy turlari.
10. Kompyuter viruslari nima?
11. Zararli dasturiy vositalardan himoyalanish usullari va vositalari.
12. Antivirus dasturiy vositalarini tanlashdagi talablar.

FOYDALANILGAN ADABIYOTLAR

1. S.K.Ganiev, T.A.Kuchkarov. Tarmoq xavfsizligi (Mobil tarmoq xavfsizligi). O‘quv uslubiy qo‘llanma. –T.: «Aloqachi», 2019, 140 b.
2. S.K.Ganiev, M.M.Karimov, Z.T.Xudoyqulov, M.M.Kadirov. Axborot xavfsizligi bo‘yicha atama va tushunchalarning rus, o‘zbek va ingliz tillaridagi izohli lug‘ati. –T.: «Iqtisod-moliya», - 2017, 480 bet.
3. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. –T.: «Fan va texnologiya», 2016, 372 bet.
4. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. Axborot-kommunikatsion tizimlar xavfsizligi. O‘quv uslubiy qo‘llanma. –T.:
«Aloqachi», 2008, 382 bet.
5. Stamp M. Information security: principles and practice // John Wiley & Sons, 2011, -P. – 606.
6. Марков А. С., Барабанов А. В., Дорофеев А. В., Цирлов В.Л. Семь безопасных информационных технологий / под ред. А.С.Маркова. –М.: ДМК Пресс, -2017. – 224с.
7. D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, I.U.Xolimtoyeva. Kriptografiyaning matematik asoslari. O‘quv uslubiy qo‘llanma. –T.: «Aloqachi», 2019, 192 bet.
8. Akbarov D.Y. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi // Toshkent, 2008, 394 bet.
9. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2017. — 416 с.
10. Raef Meeuwisse. Cybersecurity for Beginners (2nd. ed.). Cyber Simplicity Ltd, London, England, 2017, - 224 p.
11. Manjikian M. Cybersecurity ethics: an introduction. – Routledge, 2017, -328 p.
12. Kostopoulos G. Cyberspace and cybersecurity. – CRC Press, 2017, -316 r.
13. Christen M., Gordijn B., Loi M. The Ethics of Cybersecurity. – Springer Nature, 2020. – S. 384.
14. Pande J. Introduction to Cyber Security. Uttarakhand Open University, 2017, -152 p.
15. Cybersecurity Fundamentals Study Guide, ISACA 2015, -196 p.

16. Easttom C. Computer security fundamentals. – Pearson IT Certification, 2019, -447 p.

17. Введение в информационную безопасность автоматизированных систем: учебное пособие / В. В. Бондарев. — Москва : Издательство МГТУ им. Н. Э. Баумана, 2016. — 250 с.

18. Shinder D. L., Cross M. Scene of the Cybercrime. – Elsevier, 2008.

19. Scarfone K. et al. Guide to storage encryption technologies for end user devices //NIST Special Publication. – 2007. – T. 800. – S. 111.

20. Curricula Cybersecurity. Curriculum guidelines for post-secondary degree programs in cybersecurity. – 2017.

21. Purdy G. ISO 31000: 2009—setting a new standard for risk management //Risk Analysis: An International Journal. – 2010. – T. 30. – №. 6. – S. 881-886.

22. Zlatanov N. Hard Disk Drive and Disk Encryption, 2015, DOI: 10.13140/RG.2.1.1228.9681.

23. Ganiev S.K., Khudoykulov Z.T., Islomov Sh.Z., Selection suitable biometrics for cryptographic key generators // TUIT BULLETIN, Tashkent, 2016, №4 (40), – P. 80-92

24. Rathgeb C., Uhl A. A survey on biometric cryptosystems and cancelable biometrics //EURASIP Journal on Information Security, 2011, №1, – P. 1-25.

25. Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Years 2015, 2016, and 2017. U.S. Department of Health and Human Services Office for Civil Rights. https://www.hhs.gov/sites/default/files/breach-report-to-congress-2015-2016-2017.pdf

Internet manbalari

1. ACR39U smart card rader [sayt]: http://smartkardtechnologies.com/productdetails/acr39u-smart-card-rader (murojaat vaqti: 29.10.2020).

2. Certified Network Defender [sayt]: https://iclass.eccouncil.org/our-courses/certified-network-defender-cnd/ (murojaat vaqti: 29.10.2020).

3. 3D Airport Security X-ray Machine [sayt]: https://www.turbosquid.com/3d-models/3d-airport-x-ray-machine-security-1405223 (murojaat vaqti: 29.10.2020).

4. Web Applications vulnerabilities and threats: statistics for

2019 [sayt]: https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/ (murojaat vaqti: 29.10.2020).

5. How to Spot Phishing Emails [sayt]: https://www.nuigalway.ie/itsecurity/howtospotphishingemails/ (murojaat vaqti: 29.10.2020).
6. Beware of fake microsoft security essentials [sayt]: https://techjaws.com/beware-of-fake-microsoft-security-essentials/ (murojaat vaqti: 29.10.2020).
7. The Best Antivirus Protection for 2020 [sayt]: https://www.pcmag.com/roundup/256703/the-best-antivirus-protection (murojaat vaqti: 29.10.2020).
8. Securing Wireless Networks [sayt]: https://www.us-cert.gov/ncas/tips/ST05-003 (murojaat vaqti: 29.10.2020).
9. Why High Availability Is Important for Your Business [sayt]: https://blog.layershift.com/why-high-availability-for-your-business/ (murojaat vaqti: 29.10.2020).
10. Rutoken [sayt]: https://www.rutoken.ru/ (murojaat vaqti: 29.10.2020).
11. Comparison of disk encryption software [sayt]: https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software (murojaat vaqti: 29.10.2020).
12. G20 summit: NSA targeted Russian president Medvedev in London [sayt]: https://www.theguardian.com/world/2013/jun/16/nsa-dmitry-medvedev-g20-summit (murojaat vaqti: 29.10.2020).
13. CRADC Data Destruction and Return of Restricted Data Policy [sayt]: https://ciser.cornell.edu/wp-content/uploads/2017/01/CRADC_Destruction_and_Return_of_Restricted_Data.pdf (murojaat vaqti: 29.10.2020).
14. Privacy Impact Assessment Integrated Automated Fingerprint Identification System National Security Enhancements [sayt]: https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/iafis (murojaat vaqti: 29.10.2020).
15. Best Keylogger for Windows 10 in 2020 [sayt]: https://www.pctattletale.com/blog/1505/best-keylogger-software-windows-10 (murojaat vaqti: 29.10.2020).
16. Windows Event Logging and Forwarding [sayt]: https://www.cyber.gov.au/acsc/view-all-content/publications/windows-event-logging-and-forwarding (murojaat vaqti: 29.10.2020).

QISQARTMA SO‘ZLAR RO‘YXATI

ABAC - Attribute-based access control
AES - Advanced Encryption Standard
APT - Advanced persistent threats
ASSII – American Standard Code for Information Interchange
AT – Axborot texnologiyalari
CBC - Cipher Block Chaining
CCTV - Closed-circuit television
CDMA - Code Division Multiple Access
CSEC2017 JTF – Cybersecurity Curricula 2017 Joint Task Force
CVE - Common Vulnerabilities and Exposures
DAC - Discretionary access control
DES - Data Encryption Standard
DLP - Data Leakage Prevention,
DoD – Department of Defense
DOS - Denial of service
ECB - Electronic codebook mode
FAR - False Acceptance Rate
FRR - False Rejection Rate
FTP – File Transfer Protocol
GNFS - General Number Field Sieve
GSM – Global System for Mobile Communications
HMAC – hash-based message authentication code
HTTP - Hypertext Transfer Protocol
HTTPS - Hypertext Transfer Protocol Secure
IDS - Instrusion Detection System
IPS - Intrusion Prevention System
IPSec - IP Security
ISO – International Organization for Standardization
IV - Initialization Vector
KDC - Key Destribution Center
L2TP - Layer 2 Tunneling Protocol
LAN - Local Area Network
MAC - Mandatory access control
MAC - Message Authentication Code
MAN - Metropolitan Area Network
MITM - Man in the middle attack
NAT - Network Address Translation
OWASP - Open Web Application Security Project

PAN - Personal Area Network
PIN - Personal Identification Number
PKI - Public key infrastructure
PPP – Point-to-Point Protocol
PPTP - Point-to-Point Tunneling Protocol
RAID - Redundant Array of Independent Disks
RBAC - Role-based access control
RFID – Radio Frequency IDentification
SIM - Security Information Management
SSID - Service Set Identifier
SSL - Secure Sockets Layer
TCP/IP – Transmission Control Protocol/Internet Protocol
USB – Universal Serial Bus
UTM - Unifield Threat Management
VPN – Virtual Private Network
WAN - Wide Area Network
WEP - Wired Equivalent Privacy
WLAN - Wireless Local Area Network
WMAN - Wireless Metropolitan Area Network
WPA - Wi-Fi Protected Access
WPAN - Wireless Personal Area Network
WWAN - Wireless Wide Area Network
AOB - Alisaning onlayn banki
ATM – Automated teller machine
MAC - Media access control
OT – Operatsion tizim
ERI - Elektron raqamli imzo

ATAMALARNING RUS, O‘ZBEK VA INGLIZ TILLARIDAGI IZOHLI LUG‘ATI

Авторизация - представление пользователю определенных прав доступа на основе положительного результата его аутентификации в системе.
Avtorizatsiya – tizimda foydalanuvchiga, uning ijobiy autentifikatsiyasiga asosan, ma’lum foydalanish huquqlarini taqdim etish.
Authorization – granting the user certain access rights based on the positive result of authentication in the system.
Администратор защиты - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.
Himoya ma’muri – avtomatlashtirilgan tizimni axborotdan ruxsatsiz foydalanishdan himoyalashga javobgar foydalanish subyekti.
Security administrator - the subject of the access responsible for the protection of the automated system against unauthorized access to the information.
Администратор системы - лицо, отвечающее за эксплуатацию системы и поддержание ее в работоспособном состоянии.
Tizim ma’muri – tizimni ekspluatatsiyasiga va uning ishga layoqatlik holatini ta’minlashga javobgar shaxs.
System administrator – a person who is responsible for operation of the system and keeping it in an appropriate working condition.
Актив - 1. Информация или ресурсы, подлежащие защите. 2. Все, что имеет ценность для организации. 3. Главное приложение, общая система поддержки, высоко авторитетная программа, материальная часть, миссия критической систем, персонал, оборудование или логически связанная группа систем.
Aktiv - 1. Himoyalanuvchi axborot yoki resurslar. 2. Tashkilot uchun qiymatli barcha narsalar. 3. Bosh ilova, umumiy madadlovchi tizim, yuqori nufuzli dastur, moddiy qism, kritik tizim missiyasi, xodimlar, jihozlar yoki mantiqiy bog’langan tizimlari guruhi.
Asset - 1. Information or resources that should be protected. 2. Anything that has value to the organization. 3. A major application, general support

system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Активная угроза - угроза преднамеренного несанкционированного изменения состояния системы.

Faol tahdid – tizim holatini atayin ruxsatsiz o’zgartirish tahdidi.

Active threat – a threat that can make a deliberate unauthorized change to the system.

Алгоритм шифрования - алгоритм криптографический, реализующий функцию шифрования. В случае шифрсистем блочных получается использованием алгоритма шифрования блочного базового в конкретном режиме шифрования.

Shifrlash algoritmi - shifrlash funksiyasini amalga oshiruvchi kriptografik algoritm. Blokli shifrtizim holida shifrlashning muayyan rejimida shifrlashning bazaviy blokli algoritmidan foydalanib hosil qilinadi.

Encryption algorithm - a cryptographic algorithm that implements the function of encryption. In the case of block cipher system is obtained using the algorithm of the base block encryption in a particular mode of encryption.

Алгоритм криптографический - алгоритм, реализующий вычисление одной из функций криптографических.

Kriptografik algoritm – kriptografik funksiyalardan birini hisoblashni amalga oshiruvchi algoritm.

Cryptographic algorithm - the algorithm that implements the calculation of one cryptographic functions.

Алгоритм расшифрования - алгоритм криптографический, обратный к алгоритму шифрования и реализующий функцию расшифрования.

Deshifrlash algoritmi – deshifrlash funksiyasini amalga oshiruvchi va shifrlash algoritmiga teskari algoritm.

Decryption algorithm – the cryptographic algorithm which is inverse to the encryption algorithm that implements the decryption function.

Алгоритм хеширования - в криптографии - алгоритм, реализующий хеш-функцию криптографическую. В математике и

программировании - алгоритм преобразования строк символов, как правило, уменьшающий длину строки и такой, что значение каждого символа выходной строки зависит сложным образом от большого количества входных символов (в идеале - от всех). Обычно, алгоритм хеширования преобразует строки произвольной длины в строки фиксированной длины.

Xeshlash algoritmi – kriptografiyada kriptografik xesh-funksiyani amalga oshiruvchi algoritm. Matematika va dasturlashda – odatda, satr uzunligini kamaytiruvchi simvollar satrini o'zgartiruvchi algoritm. Chiqish yo'li satrining har bir simvolining qiymati kirish yo'li simvollarining katta soniga (idealda – barchasiga) murakkab tarzda bog'liq. Odatda xeshlash algoritmi ixtiyoriy uzunlikdagi satrni belgilangan uzunlikdagi satrga o'zgartiradi.

Hashing algorithm – in cryptography, an algorithm that implements the cryptographic hash function. In mathematics and computer programming - algorithm for converting strings of characters, generally reducing the length of the string and such that the value of each symbol of the output string depends in a complex way from a large number of input characters (ideally all). Usually, hashing algorithm converts strings of arbitrary length to strings of fixed length.

Алгоритм цифровой подписи - асимметричный алгоритм, используемый для цифровой подписи данных.

Raqamli imzo algoritmi - ma'lumotlarni raqamli imzolash uchun foydalaniluvchi asimetrik algoritm.

Digital signature algorithm – asymmetric algorithm used for digitally signing data.

Алгоритм шифрования RSA - алгоритм шифрования, предложенный в 1978 г. Р. Райвестом, А. Шамиром и Л. Адлеманом и предназначенный для построения шифрсистем асимметричных.

RSA shifrlash algoritmi – 1978 yili R. Rayvest, A Shamir va L.Adleman tomonidan taklif etilgan va asimetrik shifr tizimlarini qurishga mo'ljallangan shifrlash algoritmi.

RSA encryption algorithm - the encryption algorithm proposed in 1978 by R. Rivest, A. Shamir and L. Adleman and is designed to build asymmetric ciphers.

Анализ - изучение значимости полученных данных и доказательственной ценности к случаю.
Tahlil – olingan ma’lumotlarning muhimligi va vaziyat uchun isbotlanganlik qiymatini o’rganish.
Analysis – the examination of acquired data for its significance and probative value to the case.
Анализаторы сетевые (сниффер) - программы, осуществляющие «прослушивание» трафика сетевого и автоматическое выделение из трафика сетевого имен пользователей, паролей, номеров кредитных карт, другой подобной информации.
Tarmoq tahlillagichlari (sniffer) – tarmoq trafigini “tinglash”ni va tarmoq trafigidan avtomatik tarzda foydalanuvchilar ismini, parollarni, kredit kartalar nomerini, shu kabi boshqa axborotni ajratib olishni amalga oshiruvchi dasturlar.
Network analyzers (sniffer) - programs that listen on network traffic and automatic allocation of network traffic usernames, passwords, credit card numbers, and other such information.

Антивирус - программа, обнаруживающая или обнаруживающая и удаляющая вирусы. Если вирус удалить не удается, то зараженная программа уничтожается. Еще - программа, предназначенная для защиты от вирусов, обнаружения зараженных программных модулей и системных областей, а также восстановления исходного состояния зараженных объектов.
Antivirus – viruslarni aniqlovchi yoki aniqlovchi va yo’q qiluvchi dastur. Agar virus yo’q qilinmasa, zaharlangan dastur yo’q qilinadi. Yana – viruslardan himoyalashga, zaxarlangan dasturiy modullar va tizimli makonlarni aniqlashga, hamda zaxarlangan obyektlarning dastlabki holatini tiklashga mo’ljallangan dastur.
Antivirus - the program that detect or detect and remove viruses. If virus remove not possible, then the infected program is destroyed. Another program, designed to protect against viruses, detecting infected software modules and system areas as well as restore the original state of infected object.

Аппаратное средство защиты информации - специальное защитное устройство или приспособление, входящее в комплект технического средства обработки информации.
Axborotni himoyalashning apparat vositasi – axborotni ishlovchi texnik vositasi komplekti tarkibiga kiruvchi maxsus himoyalovchi qurilma yoki moslama.
Hardware data protection - a special protective device or fixture included in the kit technical tools of information processing.

Апплеты вредоносные - небольшие приложения, которые автоматически загружаются и выполняются, и которые реализуют несанкционированные функции информационной системы.
Zararli appletlar - axborot tizimida ruxsat etilmagan funksiyalarni amalga oshiruvchi, avtomatik yuklanuvchi va bajariluvchi kichik ilovalar.
Malicious applets – small application that are automatically downloaded and executed and that perform an unauthorized function on an information system.

Архитектура IT безопасности - описание принципов безопасности и общего подхода для соблюдения принципов, управляющих системой проектирования безопасности.
AT xavfsizlik arxitekturasi - xavfsizlikni loyihalash tizimini boshqaruvchi prinsiplariga rioya qilish uchun xavfsizlik prinsiplarining va umumiy yondashishning tavsifi.
IT security architecture – a description of security principles and an overall approach for complying with the principles that drive the system design.

Архитектура информационной безопасности - встроенная, неотъемлемая часть архитектуры предприятия, описывающая структуру и поведение процессов безопасности, систем информационной безопасности, персональных и организационных подразделений, с указанием их выравнивание с целью и стратегическими планами предприятия.
Axborot xavfsizligining arxitekturasi - tashkilot xavfsizlik jarayonlari strukturasi va ishlash rejimini, axborot xavfsizligi tizimlarini, shaxsiy va tashkiliy bo’linmalarini, ularni tashkilot missiyasi va strategik rejalariga tenglashtirishni ko’rsatish bilan tavsiflovchi tashkilot arxitekturasining o’rnatilgan, ajratib bo’lmas qismi.

Information security architecture – an embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.

Атака «противник в середине» — атака на протокол криптографический, в которой противник C выполняет этот протокол как с участником A, так и с участником B. Противник C выполняет сеанс с участником A от имени B, а с участником B от имени A. В процессе выполнения противник пересылает сообщения от A к B и обратно, возможно, подменяя их. В частности, в случае протокола аутентификации абонента успешное осуществление атаки «противник в середине» позволяет противнику аутентифицировать себя для B под именем A.

«Dushman o'rtada» xujumi – kriptografik protokolga hujum bo'lib, bunda dushman C ushbu protokolni ishtirokchi A va ishtirokchi B bilan bajaradi. Dushman C ishtirokchi A bilan seansni ishtirokchi B nomidan, ishtirokchi B bilan esa ishtirokchi A nomidan bajaradi. Bajarish jarayonida dushman ishtirokchi A dan ishtirokchi V ga va aksincha xabarni, ehtimol, o'zgartirib uzatadi. Xususan, abonentni autentifikatsiyalash protokoli holida «dushman o'rtada» hujumining muvafaaqiyatli amalga oshirilishi dushmanga ishtirokchi B uchun o'zini ishtirokchi A nomidan autentifikatsiyalashga imkon beradi.

Attack "the opponent in the middle" - attack on a cryptographic protocol in which the enemy with this protocol performs as a party A and party B with C. Enemy performs session with party A on behalf of B, and a participant on behalf of A. During runtime opponent forwards messages from A to B and back, possibly replacing them attacks. In particular, in the case of an authentication protocol is connected to the success of the attack "the opponent in the middle" allows authenticate itself to the enemy in the name of A.

Атака на отказ в обслуживании — атака с целью вызвать отказ системы, то есть создать такие условия, при которых легитимные пользователи не смогут получить доступ к предоставляемым системой ресурсам, либо этот доступ будет значительно затруднён.

Xizmat qilishdan voz kechishga undaydigan hujum – tizim buzilishiga sabab bo'luvchi hujum, ya'ni shunday sharoitlar tug'diradiki, qonuniy

foydalanuvchi tizim taqdim etgan resurslardan foydalana olmaydi yoki foydalanish anchagina qiyinlashadi.
Denial-of-service attack - attack intended to cause a system failure, that is, to create conditions under which legitimate users will not be able to access the system-provided resources, or this access much more difficult.

Атака пассивная — атака на криптосистему или протокол криптографический, при которой противник и/или нарушитель наблюдает и использует передаваемые сообщения шифрованные, но не влияет на действия пользователей законных.
Passiv hujum – kriptotizmga yoki kriptografik protokolga hujum bo'lib, bunda dushman va/yoki buzg'unchi uzatiluvchi shifrlangan axborotni kuzatadi va ishlatadi, ammo qonuniy foydalanuvchilar harakatiga ta'sir etmaydi.
Passive attack - attack on a cryptosystem or a cryptographic protocol in which enemy and/or the offender observes and uses the transmitted messages are encrypted, but does not affect the user's actions legitimate.

Атака со словарем паролей — атака на криптосистему, основанная на переборе значений пароля.
Parollar lug'atiga asoslangan hujum – parol qiymatlarini saralashga asoslangan kriptotizimga hujum.
Attack with a dictionary of passwords - the attack on the cryptosystem based on iterating the value of a password.

Аутентификатор - средство аутентификации, представляющее отличительный признак пользователя. Средствами аутентификации пользователя могут быть дополнительные кодовые слова, биометрические данные и другие отличительные признаки пользователя.
Autentifikator – foydalanuvchining farqli alomatini ifodalovchi autentifikatsiya vositasi. Qo'shimcha kod so'zlari, biometrik ma'lumotlar va foydalanuvchining boshqa farqli alomatlari autentifikatsiya vositalari bo'lishi mumkin.
Authenticator - means of authentication that represents the distinctive attribute of the user. Means of user authentication can be additional code word, biometric data and other identifying features of the user.

Аутентификация - проверка идентификации пользователя, устройства или другого компонента в системе, обычно для принятия решения о разрешении доступа к ресурсам системы; проверка целостности хранящихся или передающихся данных для обнаружения их несанкционированной модификации.
Autentifikatsiya – odatda tizim resurslaridan foydalanishga ruxsat etish xususida qaror qabul uchun foydalanuvchining, qurilmaning yoki tizimning boshqa tashkil etuvchisining identifikasiyasini tekshirish; saqlanuvchi va uzatuvchi ma’lumotlarning ruxsatsiz modifikatsiyalanganligini aniqlash uchun tekshirish.
Authentication - checking the identification of user, device, or other component in the system, typically for decision-making about access to system resources; check the integrity of stored or transmitted data to detect unauthorized modification.

Аутентификация биометрическая — способ аутентификации абонента (пользователя), основанный на проверке его биометрических характеристик (отпечатков пальцев, геометрии руки, лица, голоса, рисунка сетчатки глаза и т. п.). К преимуществам данного метода относится неотделимость биометрических характеристик от пользователя: их нельзя забыть, потерять или передать другому пользователю.
Biometrik autentifikatsiya – abonentni (foydalanuvchini) uning biometrik xarakteristikasi (barmoq izlari, panja geometriyasi, yuzi, ovozi, ko’z pardasining to’ri va h.) asosidagi autentifikatsiyalash usuli. Ushbu usulning afzalligi – biometrik xarakteristikalarni foydalanuvchidan ajratib bo’lmasligi. Ularni esdan chiqarishning, yo’qotishning yoki boshqa foydalanuvchiga berishning iloji yo’q.
Biometric authentication - the method of authentication of a subscriber (user), based on a verification of biometric characteristics (fingerprints, hand geometry, face, voice, eye retina image, etc.). The advantages of this method is the inseparability of biometric characteristics from user: they cannot be forgotten, lost or transferred to another user.

Аутентификация двухфакторная — аутентификация пользователей на основе двух разнородных факторов, как правило, на основе того, что знает пользователь, и того, чем он владеет (например, на основе пароля и физического идентификатора).

Ikki faktorli autentifikatsiya – foydalanuvchilarni ikkita turli faktorlar asosida autentifikatsiyalash, odatda, foydalanuvchi biladigan narsa va egalik qiladigan narsa (masalan, parol va fizik identifikatori) asosida.
Two-factor authentication - user authentication on the basis of two unrelated factors, as a rule, on the basis of what he knows and what he knows (e.g., password-based and physical ID).

Аутентификация на основе паролей одноразовых — технология аутентификации с помощью паролей одноразовых, для получения которых могут использоваться: алгоритм генерации на основе односторонней функции, специальные устройства – токены, либо технология OOB (out of band), основанная на передаче пароля одноразового с использованием дополнительного канала, отличного от того, по которому пользователь осуществляет доступ к прикладной системе.
Bir martali parollar aosidagi autentifikatsiya - bir martali parollar yordamida autentifikatsiyalash texnologiyasi. Bir martali parollarni olishda quydagilar ishlatilishi mumkin: bir tomonlama funksiya asosida generatsiyalash algoritmi, maxsus qurilmalar-tokenlar, yoki bir martali parolni, foydalanuvchi tatbiqiy tizimdan foydalanishda ishlatiladigan kanaldan farqli, kanal orqali uzatishga asoslangan OOB (out of band) texnologiyasi.
One time password based authentication - technology authentication using one time passwords, which can be used: the generation algorithm based on one-way functions, special device – taken, or technology OOB (out of band) based on the transmission password disposable using additional channels, other than where the user accesses the application system.

Аутентификация сообщений - добавление к блоку данных контрольного поля для обнаружения любых изменений в данных. При вычислении значений этого поля используется ключ, известный только приемнику данных.
Xabarlar autentifikatsiyasi – ma’lumotlarda har qanday o’zgarishlarni aniqlash maqsadida ma’lumotlar blokiga nazorat hoshiyasini qo’shish. Ushbu hoshiya qiymatini hisoblashda faqat ma’lumotlar priyemnigiga ma’lum kalitlar ishlatiladi.

Message authentication - adding control data to the data field to detect any changes in the data. The values of this field using a key known only to receiver data.

База данных - совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ. Является информационной моделью предметной области. База данных, как правило, представляются тремя уровнями абстракции: внешним, концептуальным и внутренним.

Ma'lumotlar bazasi - tatbiqiy dasturlarga bog'liq bo'lmagan holda ma'lumotlarni tavsiflashning, saqlashning va manipulyatsiyalashning umumiy prinsiplarini ko'zda tutuvchi, ma'lum qoidalar bo'yicha tashkil etilgan ma'lumotlar majmui. Predmet sohasining informatsion modeli hisoblanadi. Ma'lumotlar bazasi odatda abstraksiyaning tashqi, konseptual va ichki satxlari orqali ifodalanadi.

Database - a collection of data organized according to certain rules, providing general principles for describing, storing and manipulating data independent of the application programs. An information domain model. The database, usually presented in three levels of abstraction: external, conceptual and internal.

Безопасность - свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение. Еще - состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифицированы неавторизованными лицами (включая персонал системы), компьютерами или программами.

Xavfsizlik - ta'siri natijasida nomaqbul holatlarga olib keluvchi atayin yoki tasodifiy, ichki va tashqi beqarorlovchi faktorlarga qarshi tizimning tura olish xususiyati. Yana - ma'lumotlar fayllarining va dasturlarning avtorizatsiyalanmagan shaxslar (jumladan tizim xodimi), kompyuterlar yoki dasturlar tomonidan ishlatilishi, ko'rib chiqilishi va modifikatsiyalanishi mumkin bo'lmagan holat.

Security - the property of a system to withstand external or internal destabilizing factors, the effect of which may be unwanted state or behaviour. Still - a state in which the data files and programs may not be

used, viewed and modified by unauthorized persons (including the system staff), computers or software.

Безопасность информации - состояние информации, при котором исключаются случайные или преднамеренные несанкционированные воздействия на информацию или несанкционированное ее получение; еще - состояние уровня защищенности информации при ее обработке техническими средствами, обеспечивающее сохранение таких ее качественных характеристик (свойств) как секретность (конфиденциальность), целостность и доступность.
Axborot xavfsizligi - axborot holati bo'lib, unga binoan axborotga tasodifiy yoki atayin ruxsatsiz ta'sir etishga yoki ruxsatsiz uning olinishiga yo'l qo'yilmaydi; yana - axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta'minlovchi axborotning himoyalanish darajasi holati.
Information security - status information, which excludes accidental or deliberate tampering or unauthorized information receive it, also - the state of security level information when processing technical means to ensure the preservation of its quality characteristics (properties) such as secrecy (confidentiality), integrity, and availability.

Безопасность информационная общества - то же, что и «безопасность, информационная личности» применительно к организованному коллективу людей и к обществу в целом.
Jamiyat axborot xavfsizligi – "shaxs axborot xavfsizligi" kabi, uyushgan odamlar kollektiviga va umuman, jamiyatga qo'llaniladi.
Society information security - what "safety information personality" when applied to organized team of people and to society as a whole.

Безопасность информационной сети - меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов.
Axborot tarmog'i xavfsizligi – axborot tarmog'ini ruxsatsiz foydalanishdan, me'yoriy harakatlariga tasodifiy yoki atayin aralashishdan yoki komponentlarini buzishga urinishdan saqlash choralari.

Network security - measures that protect the information network from unauthorized access, accidental or deliberate interference in normal activities or attempts the destruction of its components.

Брандмауэр - метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля за ним аппаратно-программными средствами; еще - является защитным барьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра).
Tarmoqlararo ekran – apparat-dasturiy vositalar yordamida tarmoqdan foydalanishni markazlashtirish va uni nazoratlash yo'li bilan tarmoqni boshqa tizimlardan va tarmoqlardan keladigan xavfsizlikka tahdidlardan himoyalash usuli; yana - bir necha komponentlardan (masalan, tarmoqlararo ekran dasturiy ta'minoti ishlaydigan marshrutizator yoki shlyuzdan) tashkil topgan ximoya to'sig'i hisoblanadi.
Firewall - a method of protecting a network against security threats from other systems and networks, through centralizing network access and control hardware and software; - is a protective barrier consisting of several components (e.g., router or gateway running firewall software).

Кибер инфраструктура - включает электронную информацию и коммуникационные системы, и службы и информацию, содержавшуюся в этих системах и службах.
Kiber infrastruktura – elektron axborot, kommunikatsiya tizimlari, xizmatlar va bu tizimlar va xizmatlarda mavjud axborotni o'z ichiga oladi.
Cyber infrastructure – includes electronic information and communications systems and services and the information contained in these systems and services.

Кибер инцидент - действия, использующие компьютерные сети, приводящие к фактическому или потенциальному ущербу в информационной системе и/или содержащейся в ней информации.
Kiber insident – axborot tizimi va/yoki undagi axborotga aniq yoki potensial zarar yetkazilishiga sabab bo'luvchi, kompyuter tarmoqlaridan foydalanuvchi harakatlar.
Cyber incident – actions taken using computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

Кибер-атака - атака, через киберпространство, предназначенная для использования предприятием киберпространства в целях, отключения, уничтожения или злонамеренного контроля вычислительной среды/инфраструктуры**.**
Kiber-hujum – hisoblash muhiti/ infrastrukturasini, o'chirish, buzish yoki g'arazli nazoratlash yoki ma'lumot yaxlitligini buzish yoki nazoratlanuvchi axborotni o'g'irlash maqsadida kiberfazodan foydalanuvchi tashkilotga atalgan kiberfazo orqali amalga oshiriluvchi hujum.
Cyber-attack – an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disabling, destroying, or maliciously controlling a computing environment/infrastructure.

Кибербезопасность - возможность охранять или защитить использование киберпространства кибератаками.
Kiberxavfsizlik – kiberfazoning kiberhujumlardan foydalanishidan qo'riqlash yoki himoyalash imkoniyati.
Cybersecurity – the ability to protect or defend the use of cyberspace from cyber-attacks.

Киберпреступность — действия отдельных лиц или групп, направленные на взлом систем компьютерной защиты, на хищение или разрушение информации в корыстных или хулиганских целях.
Kiberjinoyatchilik - g'arazli yoki xuliganlik maqsadlarida himoyalashning kompyuter tizimlarini buzib ochishga, axborotni o'g'irlashga yoki buzishga yo'naltirilgan alohida shaxslarning yoki guruhlarning harakatlari.
Cyber cryme — the actions of individuals or groups aimed at cracking computer security systems, theft or destruction of information for selfish or destructive purposes.

Киберпространство - глобальный домен в информационной среде, состоящий из взаимозависимой сети инфраструктур информационных систем включая Интернет, сети телекоммуникации, компьютерные системы, и встроенные процессоры и контроллеры.
Kiberfazo – Internet, telekommunikatsiya tarmoqlari, kompyuter tizimlari va o'rnatilgan prosessorlar va kontrollerlarni o'z ichiga olgan,

o’zaro bog’langan axborot tizimlari infrastrukturalar tarmog’idan tashkil topgan axborot muhitidagi global domen.
Cyberspace – a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Кибертерроризм — действия по дезорганизации компьютерных систем, создающие опасность гибели людей, значительного имущественного ущерба либо иных общественно опасных последствий.
Kiberterrorizm - insonlar halokati, aytarlicha moddiy zarar xavfini yoki boshqa jamiyatga xavfli oqibatlarni tug’diruvchi kompyuter tizimlarini izdan chiqarish bo’yicha harakatlar.
Cyber terrorism — action disruption of computer systems, creating a danger of loss of life, significant property damage or other socially dangerous consequences.

Привилегии - права пользователя или программы, состоящие в доступности определенных объектов и действий в вычислительной системе.
Imtiyozlar - hisoblash tizimida ma’lum obyektlardan foydalanish va ularda ishlashdan iborat foydalanuvchilarning yoki dasturning huquqlari.
Privilege - rights of the user or a program, consisting in the availability of certain objects and actions in a computing system.

Приложение – программное обеспечение (программа) информационной системы, выполняющая определенную функцию непосредственно для пользователя без доступа к системе управления, мониторинга или административным привилегиям.
Ilova – bevosita foydalanuvchi uchun boshqarish, monitoringlash tizimlaridan yoki ma’muriy imtiyozlardan foydalanmay aniq funksiyani bajaruvchi axborot tizimining dasturiy ta’minoti (dasturi).
Application – a software (program) hosted by an information system. In addition, software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.

Программа антивирусная — программа компьютерная, предназначенная для защиты от вирусов компьютерных. Осуществляет обнаружение, восстановление, блокирование и/или удаление зараженных программных модулей и системных областей.
Virusga qarshi dastur - kompyuter viruslaridan himoyalashga mo'ljallangan kompyuter dasturi. Zaharlangan dasturiy modullarni va tizim sohalarini aniqlashni, tiklashni, blokirovka qilishni va/yoki yo'q qilishni amalga oshiradi.
Antivirus program - a computer program designed to protect the viruses from the computer. Detection, recovery, blocking and/or deleting infected software modules and system areas.

Виртуальная частная сеть - виртуальная сеть, построенная на основе существующих физических сетей, обеспечивающая безопасный туннель коммуникации для передачи данных или другой информации, передаваемой между сетями.
Virtual shaxsiy tarmoq - tarmoqlar orasida almashiniluvchi ma'lumotlar yoki boshqa axborotni uzatish uchun xavfsiz kommunikatsiya tunnelini ta'minlovchi, mavjud fizik tarmoqlar asosida qurilgan virtual tarmoq.
Virtual private network – a virtual network, built on top of existing physical networks that provides a secure communications tunnel for data and other information transmitted between networks.

Контроль доступа на основе ролей - модель для управления доступом к ресурсам, когда разрешенные действия на ресурсы идентифицированы с ролями, а не с личными идентификаторами субъекта.
Rollarga asoslangan ruxsatni nazoratlash - resurslardan foydalanishni boshqarish modeli bo'lib, resurslarda ruxsat berilgan harakatlar shaxsiy subyekt identifikatorining o'rniga rollar bilan identifikatsiyalanadi.
Role-based access control – a model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.

Конфиденциальность – 1. Некоторый класс данных, получение либо использование которых неавторизованными для этого лица не может стать причиной серьезного ущерба для организации. 2. Свойство информации, состоящее в том, что она не может быть

обнаружена и сделана доступной без разрешения отдельным лицам, модулям или процессам.
Konfidensiallik – 1. Avtorizatsiyalanmagan shaxs tomonidan olinishi yoki foydalanishi tashkilot uchun jiddiy zarar sababi bo'la olmaydigan ma'lumotlarning qandaydir sinfi. 2. Alohida shaxslar, modullar, jarayonlar ruxsatisiz aniqlanishi, va foydalanishi mumkin bo'lmagan axborot xususiyati.
Confidentiality – 1. Some class data, obtaining or the use of which by unauthorized persons could not cause serious damage to the organization. 2. The quality of information, consisting in that it cannot be detected and made available without the permission of individuals, modules or processes.

Менеджмент риска — полный процесс идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы информационно-телекоммуникационных технологий.
Risk menejmenti — axborot-telekommunikatsiya texnologiya resurslariga ta'sir etishi mumkin bo'lgan xavfli xodisalar oqibatlarini identifikatsiyalashning, nazoratlashning, bartaraf etishning yoki kamaytirishning to'liq jarayoni.
Risk management — the complete process of identification, control, eliminate or mitigate the consequences of hazardous events that may affect resources of information and telecommunication technologies.

Целостность - свойство информации, заключающееся в её существовании в неискаженном виде (неизменном по отношению к некоторому физическому её состоянию).
Yaxlitlik - axborotning buzilmagan ko'rinishda (axborotning qandaydir fizik holatiga nisbatan o'zgarmagan shaklda) mavjud bo'lishida ifodalangan xususiyati.
Integrity - the property of information, namely, its existence in an undistorted view (unchanged with respect to some physical condition).

MUNDARIJA